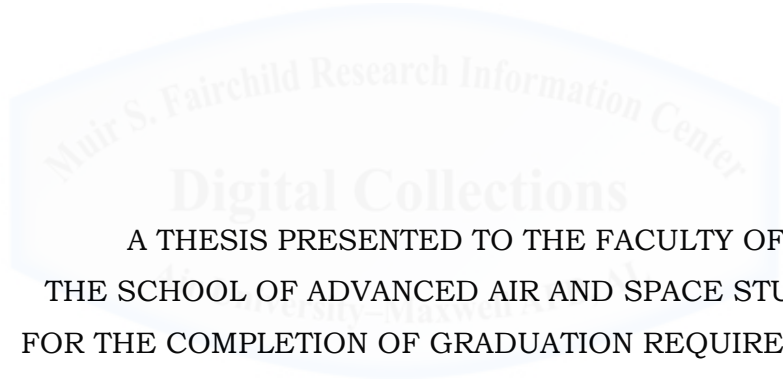


CENTRALIZED OFFENSE, DECENTRALIZED DEFENSE:
COMMAND AND CONTROL OF CYBERSPACE

BY
AARON M. GIBNEY



A THESIS PRESENTED TO THE FACULTY OF
THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES
FOR THE COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES
AIR UNIVERSITY
MAXWELL AIR FORCE BASE, ALABAMA
JUNE 2012

APPROVAL

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

COL MELVIN DEALE (Date)

COL SUZANNE BUONO (Date)



DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.



ABOUT THE AUTHOR

Major Aaron M. Gibney earned a Bachelor of Arts degree in history as a 1999 graduate of Indiana University. He was commissioned through the Air Force Reserve Officer Training Corps' Detachment 215, and his first duty station was Tyndall Air Force Base, Florida, where he attended Undergraduate Air Battle Manager (ABM) Training. His initial ABM assignment was at Robins AFB, Georgia where he flew as an Air Weapons Officer aboard the E-8C Joint Surveillance Target Attack Radar System aircraft. Following a one-year remote to Iceland, Maj. Gibney returned to Robins and, in 2006, graduated from the Air Force Weapons School, Class 06BIC. During his time at Robins, he deployed multiple times in support of OEF and OIF. He is a Senior Air Battle Manager with over 1,600 flying hours and almost 700 combat hours.

In the fall of 2008, Maj. Gibney returned to Tyndall to instruct at the ABM schoolhouse. There he served as the Chief of Wing Weapons and Tactics in the 325 Fighter Wing and as the Assistant Operations Officer for the 325 Air Control Squadron. During Maj. Gibney's time at Tyndall, he revamped the Undergraduate Air Battle Manager syllabus to create AETC's first non-pilot or navigator wings awarding course.

Maj. Gibney graduated from Air Command & Staff College, and following graduation from the School of Advanced Air and Space Studies will be assigned to Ramstein Air Base, Germany where he will serve as the Chief of Strategy Plans at the 603 Air Operations Center.

Digital Collections
Air University—Maxwell AFB, AL

ACKNOWLEDGEMENTS

This year has been one of the most challenging and rewarding of my career. First, I want to thank my joint and coalition SAASS XXI classmates. I am honored to call them comrades-in-arms and friends. I would also like to acknowledge the faculty and staff of SAASS, a group of individuals whose level of academic professionalism and dedication has yet to be surpassed in my 13-year military career.

I would also like to specifically acknowledge several people without whose help I would never have gotten this study off the ground. My sincere thanks go to Dr. John Sheldon who provided my initial guidance into this strategic journey, and Colonel Dean Clothier who provided me with the insight necessary to focus this effort. Certain thanks go to Colonel Suzanne Buono for her exceptional instruction in the cyber course and her rare ability to provide constructive criticism throughout my writing process. I especially want to thank my research advisor, Colonel Melvin Deaile, for his invaluable insight, advice, and mentoring throughout the course of this project. Without his prodding, prompting, and editorial destruction of my initial drafts, this investigation would have fallen short of its intended goal.

Most importantly, I want to express my sincere appreciation to my family for their patience and understanding during those times when I was physically or mentally absent while completing this project. Without their support and unconditional love this paper would not have been possible.

ABSTRACT

Shortly after World War II, the same group of individuals that created an “end-of-the-world” weapon developed another technology that created the beginning of a new world. This new world technology was the computer, and the new domain of cyberspace soon followed. The transfer of information by electronic means is not new. Cyberspace has proven to be another giant leap forward in command technology.

Attack in cyberspace is often over exaggerated, more commonly resembling vandalism, voyeurism, spying, or petty theft. But with the nation’s and the military’s reliance on this domain growing, the strategic implications of cyberspace cannot be ignored. Commanders must operate in this environment with the control and authorities necessary to shield themselves from attacks, stop the attackers, repair their networks, and continue to fight while all this occurs. This capability should be provided to Joint Force Commanders (JFCs) by means of an Area Cyber Defense Commander (ACDC) whose responsibilities will include developing and executing an area of responsibility’s (AOR’s) cyber defense plan.

The offensive use of cyber travels beyond one’s own network. This unique situation requires a global command center that can provide cyber situational awareness (SA) and command and control (C2) of long-range cyber fires. This model should be established under Cyber Command (CYBERCOM) and provide JFCs and ACDCs with the guidance necessary if cyber attack is needed. The Strategic Area Cyber Center (SACC) will allow for the centralized C2 of offensive cyber.

Commanders should have inherent authorities and capacities to stop these attacks from happening; and, they should do this all the while understanding that action beyond their own networks will occur in an environment that requires strict rules and specific controls often held by a single strategic cyber commander.

CONTENTS

| Chapter | | Page |
|---------------|--|------|
| | DISCLAIMER | ii |
| | ABOUT THE AUTHOR | iii |
| | ACKNOWLEDGEMENTS | iv |
| | ABSTRACT | v |
| | INTRODUCTION | 1 |
| 1 | CYBER PRIMER | 7 |
| 2 | CYBER ORGANIZATION | 31 |
| 3 | CYBER DEFENSE—DECENTRALIZED C2 | 51 |
| 4 | CYBER OFFENSE—CENTRALIZED C2 | 71 |
| | CONCLUSION & RECOMMENDATIONS | 89 |
| | BIBLIOGRAPHY | 99 |
| ILLUSTRATIONS | | |
| Figure | | |
| 1 | World's Population Online | 11 |
| 2 | Growth of Internet Users Per 100 Inhabitants | 12 |
| 3 | Cyber War | 20 |
| 4 | Level of Danger from Cyber Threats | 22 |
| 5 | Levels of Cyber Power | 23 |
| 6 | The Global Information Grid | 37 |
| 7 | AFCYBER Proposed Organizational Chart | 41 |
| 8 | USCYBERCOM Organizational Chart | 45 |
| 9 | Cyber Power – Passive Defense | 57 |
| 10 | Cyber Power – Active Defense | 60 |

| | | |
|----|--|----|
| 11 | Cyber Defense Lines of Operation | 62 |
| 12 | ACDC Responsibilities | 63 |
| 13 | Joint ACDC Component Commander Under the JFC | 65 |
| 14 | Joint ACDC Non-Component Commander | 67 |
| 15 | ACDC Command Relationships | 70 |
| 16 | Offensive Lines of Operation | 77 |
| 17 | Cyber Attack Operations | 84 |
| 18 | Capabilities Provided by SACC | 88 |
| 19 | Cyber Power – Cyber Attack | 89 |
| 20 | Levels of Cyber Power | 92 |
| 21 | Cyber Lines of Operation | 94 |
| 22 | Levels of Cyber C2 | 96 |
| 23 | Separate Levels of Cyber Power | 97 |

Introduction

Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts . . . A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace [sic] of the mind, clusters and constellations of data. Like city lights, receding into the distance . . .

—William Gibson, *Neuromancer*

Why is cyberspace unique? A strategist's search for an answer to this question could possibly take longer than their life allows, still this paper will explore this theme. This intellectual trip should be satisfying to the strategist and reveal important and relevant particularities of cyberspace, command, and war. The world has become increasingly dependent on the flow of information in cyberspace. In fact, it has been estimated that every two days humans create as much information as was created from the dawn of civilization up until 2003.¹ Those who can control and manipulate this growth will gain and maintain power. In order to gain and maintain the advantage in cyberspace, the military must ensure the security of its information networks and, when necessary, attack the networks of its enemies. Recently, the military has taken steps to control this new domain, but questions of authorities, command and control (C2), and relationships still exist. C2 of cyber is ambiguous at best, raising yet another question: *Is the United States military developing the C2 capabilities necessary to defend its networks, and conduct strategic operations in cyberspace?*

¹ M.G. Siegler, "Eric Schmidt: Every 2 Days We Create As Much Information As We Did Up To 2003," (TechCrunch, 4 August 2010), <http://techcrunch.com/2010/08/04/schmidt-data/> (accessed 15 May 2012).

The cyber age is here, but the electronic transfer of information has been here for years.² Electricity was “captured” in the early 1800s and only a couple of decades later militaries used the wired telegraph to transmit information electronically over long distances. By the late 1800s, scientists were perfecting wireless telegraphy (radio) technology. During World War II, militaries used radar devices to transmit and receive electromagnetic waves. In the 1960s, computer scientists in America were creating technologies that would one day become the Internet, and by the turn of the 20th century, this wired network expanded globally and gained prominence in telecommunication, education, banking, and military operations. Electronically based information exchange has existed now for two centuries, and its strategic significance remains integral to US military operations. The advent of the Internet and the US military’s use of cyberspace have brought greater complexities and greater opportunities to the battlefield. Nations often make war in the same way they make wealth—each new wave of innovation and advancement in technology brings new methods of military power.³

On 3 January 2012, President Obama released his strategic guidance to the Department of Defense (DOD), proclaiming that the US would continue to invest in the capabilities critical to “prevailing in all domains, including cyber.”⁴ Secretary of Defense Leon Panetta emphasized cyber’s importance by saying the US was at a “strategic turning point,” and effectively operating in the cyber domain will preserve the military’s ability to protect America’s “core national interests.”⁵ The document continued, “Modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication

² Chapter 1, *Cyber Primer*, will define cyber.

³ Antoine Bousquet, *The Scientific Way of Warfare—Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), 216.

⁴ Department of Defense, “2012 Defense Strategic Guidance—Sustaining US Global Leadership: Priorities for 21st Century Defense,” (Washington DC, January 2012), 3.

⁵ DOD, “2012 Defense Strategic Guidance,” 4.

networks and assured access to cyberspace.”⁶ This strategic guidance highlighted America’s reliance on and the increasing importance of cyberspace. In fact, these operations are believed to be so important that cyber is one of the only areas in the DOD that is receiving an increase in budgetary funds.⁷

America’s reliance on cyberspace is well known, but the nature of cyberspace and the command and authorities of cyber power are not well established. Cyberspace is used in all aspects of warfare and supports all other instruments of power. This technology provides the US with a significant advantage over its adversaries, but it also empowers those adversaries and introduces critical vulnerabilities into the strategic equation. Cyberspace is different because it enables opponents like never before. The ease of entry into cyberspace “has enabled would-be hidden, distant, or small scale opponents to attempt societal disruption that historically only close neighbors or superpowers could consider.”⁸ Cyberspace encompasses all levels of war and must be critically examined for the strategist to properly utilize its advantages in planning and future war.

Research Questions

To gain a clearer view of cyberspace this paper will draw out a number of issues. This thesis answers the following questions: Why is cyberspace unique? How does the military organize its cyber power, and how should C2 of cyber power be conducted? In assessing these issues, this paper will map out the key options the DOD can take to utilize cyberspace to gain a strategic advantage.

⁶ DOD, “2012 Defense Strategic Guidance,” 11.

⁷ DOD, “2012 Defense Budget Priorities and Choices,” (Washington DC, January 2012), 9.

⁸ Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, GA: University of Georgia Press, 2011), 2.

The development of cyberspace has *not* changed the nature of war. What cyberspace *has* done is change the way information exchange in war is amplified. Overall, this material articulates the underlying theme: the unique domain of cyberspace requires the centralized C2 of offensive and decentralized C2 of defensive cyber capabilities. The cyber domain has allowed adversaries across the globe an easy avenue to attack America's military networks on a daily basis requiring the command and control of defensive cyber forces to rest in the hands of operational commanders. The global networked nature of cyberspace has allowed the implications of offensive attack to grow to strategic levels requiring the C2 of offensive cyber power to rest above the Combatant Command (COCOM) level.

Outline

Chapter One, *Cyber Primer*, lays out the broad conceptual framework of this study, and the foundations it rests upon. The origins of cyberspace must be examined in order to understand its nature, characteristics, and the context in which it currently resides. Ideas and definitions related to cyberspace are introduced and expanded upon to prepare the reader for the chapters that follow. In order to begin the strategic journey into cyberspace, one must understand the popular and official definitions of cyberspace, how the military uses cyber power, and what cyber is and is not in war. These basics lay the foundations for the discussion of cyber's significance.

The second chapter, *Cyber Organization*, begins by examining the unified command plan that defines the organizational structure in which cyber power has been placed. Next, this chapter looks at Strategic Command (STRATCOM) and the Air Force's efforts to control cyberspace before Cyber Command (CYBERCOM) was established. Finally,

CYBERCOM is analyzed to provide the reader with an understanding of how America defends herself in and through cyberspace.

After examining the military's framework of cyberspace, this paper will explore the C2 of defensive and offensive cyberspace capabilities. Chapter Three, *Cyber Defense—Decentralized Command and Control*, examines the vulnerability of expeditionary networks, and the DOD plan to defend them. Proper C2 of cyber defense is the answer, and this chapter will define what C2 of defense should look like. Defense of expeditionary networks will provide functionality for the commander to detect whether or not their network is under attack, and will direct a proper reaction. COCOMs currently have Network Control Centers (NCC) inherent to their operations, but they do not have an active defense capability, nor the cyber sensors and forces necessary to truly defend their networks. In order to protect their networks, COCOMs must have an inherent cyber defense capability and establish relationships with network defenders at CYBERCOM. In search for a parallel C2 architecture, the Area Air Defense Commander (AADC) will be used as a case study to compare roles and relationships relying heavily on Joint Publication 3-01, *Joint Doctrine for Countering Air and Missile Threats*, and Joint Publication 3-30, *Command and Control for Joint Air Operations*. This chapter will propose the establishment of an Area Cyber Defense Commander (ACDC) that will control cyber defense forces in theater, and provide supported and supporting "reach back" to CYBERCOM.

With this background, the fourth chapter, *Cyber Offense—Centralized Command and Control*, examines attack and exploitation in cyberspace. The C2 of offensive cyberspace must provide the capabilities to orchestrate long-range cyber fires in support of combatant commanders (CCDRs). This chapter proposes the implementation of a Strategic Attack Cyber Center (SACC), and will compare this proposed

entity to the current functions of Joint Special Operations Task Forces (JSOTF) and the Joint Space Operations Center (JSPOC). These functions include the Director of Space Forces (DIRSPACEFOR), the space advisor to the Joint Forces Air Component Commander (JFACC), space report requests, and special operations and space liaison officers (LNOs). Chapter Four relies heavily on Joint Publication 3-05, *Special Operations*, and Joint Publication 3-14, *Space Operations*.

Overall Recommendation

This thesis concludes with two overall recommendations. First, the security of vulnerable expeditionary networks requires the decentralized control of defensive cyber capabilities through the introduction of a new component commander, the ACDC. Second, the DOD must establish a structure that allows for unified C2 of long-range strategic offensive cyber attack and exploitation, specifically the SACC. With these ideas in mind, strategists can limit their vulnerabilities and cultivate their advantages of cyberspace.

Chapter 1

Cyber Primer

. . . with the wild rush of change in the pace, scope, materials, scale, and possibilities of human life that then occurred, the old boundaries, the old seclusions and separations were violently broken down. All the old settled mental habits and traditions of men found themselves not simply confronted by new conditions, but by constantly renewed and changing new conditions. They had no chance of adapting themselves. They were annihilated or perverted or inflamed beyond recognition.

—H.G. Wells, *The War in the Air*

The cyber age is here! This proclamation is being shouted from the highest mountaintop. In 1907, H.G. Wells warned of abrupt changes brought about by the “scientific age.” Today, in the “cyber age,” the strategic mind is at risk of being unable to adapt to constantly “changing new conditions.”¹ Cyber is an evocative term but because of the lack of substance and understanding it has also become distracting, especially to the military strategist. It has grown beyond just a buzzword and is now so commonly used that it has almost lost any true meaning—at the very least—it has lost its substance. At best, the term cyber is used in an attempt to stir the emotions of an audience and, at worst, it is the underlying foundation of a fear monger’s argument. Cyber is and will continue to be an increasingly popular concept when executing military operations and adapting to military problems, especially its command and control.

This chapter will move the conversation from the mountaintop down to sea level where higher oxygen levels prevail, and lead to a more reasonable and realistic argument. It will provide the strategist with the information—rather than the affirmation—required to make sound

¹ H.G. Wells, *The War in the Air* (Charleston, SC: BiblioBazaar, 1907), 82.

military judgments concerning cyber. After all, strategists must be able to separate the “cyberwheat” from the “cyberchaff” and articulate sound arguments when confronted by “cyberlittles.”² Military strategists must be aware of the incredible complexities of cyber, understand how to use and command it, and not become enamored with the temptations to make it something it is not. The nature of war remains the same with or without cyber, but cyber has changed the amplification of war.

This chapter includes four sections: cyberspace, cyber power, cyber war, and cyber strategy. These sections lay out the fundamental information necessary to begin the strategic journey of an understanding of cyberspace. The first section provides a definition of cyberspace and an explanation of its nature. The second examines cyber power and the military challenges that come with this domain. The third section explains war with and in cyber. The final section examines how cyber affects strategy. With the help of this chapter, cyber will no longer be something to fear, and strategically minded individuals will be able to protect themselves from becoming “perverted . . . beyond recognition.”³

Cyberspace

Those interested in the future of the country, not only from a national defense standpoint but from a civil, commercial and economic one as well, should study this matter carefully, because air power has not only come to stay but is, and will be, a dominating factor in the world's development.

—William “Billy” Mitchell, *Winged Defense*

Bold and extravagant claims of “cybergeddon” should remind aviation-oriented individuals of the dawn of air power. In 1907, H. G. Wells warned of German attacks against America from airships launched

² These “cyber-words” have been added to emphasize just how ridiculous the terminology can get. This paper will provide the reader with a “cyber-radar” or “cyber-shield” to use when confronted with information littered with erroneous “cyber-jargon.”

³ Wells, *The War in the Air*, 82.

across the Atlantic in his novel *The War in the Air*. Now, more than 100 years after these prophetic assertions, a new breed of Chicken Littles is warning America, especially its military, that the Internet is falling. Instead of Zeppelin attacks from the air, the exaggerated threat is an unidentifiable boogiemer with almost limitless powers inside cyberspace. While one should dismiss the images of cyber as the ultimate battlespace, one should not dismiss the utility of innovation in cyber. The godfather of American air power, General William “Billy” Mitchell, did not take innovations lightly. He believed that the new air domain was *the* key to America’s future power and sovereignty. While cyber war may not bring a Wellsian-end to civilization, Mitchell’s comments about air power hold true to cyber today. Cyber should not be feared—it should be embraced. Although strategists should draw parallels between cyber power and air power, cyberspace is a domain all its own. Cyber is here to stay and has become the dominating factor in not just the world’s development but in military development and strategic thought as well.

The origins of the concept of cyberspace can be traced to science fiction and popular culture. Overall, cyberspace has come to be known as a complex electronic environment, like the Internet. Science fiction author William Gibson, in his 1984 novel *Neuromancer*, coined the term “cyberspace,” and defined it as a “consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts.”⁴ This describes cyberspace as an everyday environment that connects large groups of people around the world and allows them to share experiences beyond what the normal world makes available. Gibson continues that cyberspace is “a graphic representation of data abstracted from banks of every computer in the human system.”⁵ Here Gibson highlights the vast amount of information this environment makes available to the masses. He finishes his

⁴ William Gibson. *Neuromancer* (New York: The Berkley Publishing Group, 1984), 51.

⁵ Gibson. *Neuromancer*, 51.

explanation by emphasizing the “unthinkable complexity,” concluding that cyberspace should be compared to the “lines of light ranged in the nonspace [sic] of the mind, clusters and constellations of data. Like city lights, receding into the distance.”⁶ Gibson clearly foresaw the vastness that would define this new environment. Gibson’s definition of cyberspace meant incredible amounts of people sharing vast amounts of information in an electronic environment almost too large to comprehend. Science fiction and poetics aside, this was an incredibly accurate prophecy.

The Internet

The Internet is the largest, most popular, and most familiar vehicle for traversing cyberspace. Gibson’s vision of the future—where billions of people from every nation connect and share information through an electronic environment—was not far from the realities of cyberspace today. Today, the world’s population has exceeded seven billion, and the Internet is the structural framework that allows a large percentage of these people to share information electronically and on a global scale. The Internet is an open system and supports numerous networks and applications—the two most popular being the World Wide Web and e-mail. In 2001, there were fewer than half a billion Internet users. Since then, that number has steadily grown, and today, that number has topped 2.4 billion.⁷ This means that a third of the world’s population now uses the Internet.

⁶ Gibson, *Neuromancer*, 51.

⁷ The total world population was almost two and a half billion as recently as the end of WWII. International Telecommunications Union, “International Communications Technology Statistics,” <http://www.itu.int/ITU-D/ict/statistics/> (accessed 20 February 2012).

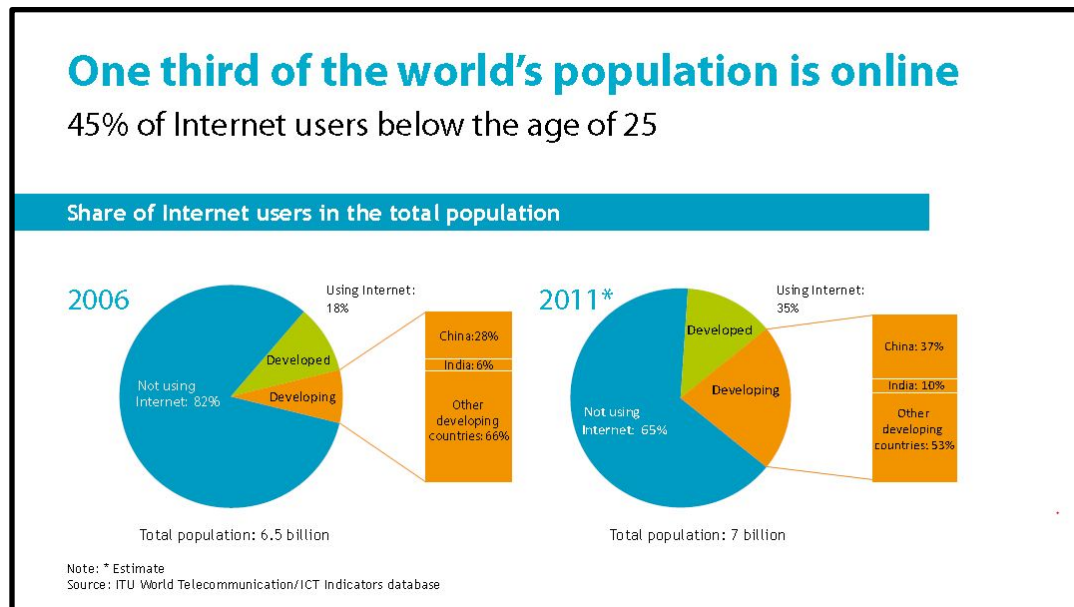


Figure 1: World's Population Online

Source: International Telecommunications Union, www.itu.int

The use of and reliance upon the Internet has not been limited to developed countries. Under-developed and developing countries are growing at the same, if not a higher rate, than developed countries.⁸ Internet technology is providing people inexpensive and consistent electronic access to the world by amplifying and accelerating their ability to communicate, share, exchange, and sell information. While this increase in Internet use is impressive, one must remember that its beginnings were shaped by a few US government researchers and academics shortly after the invention of the computer.

⁸ The world is home to seven billion people, one third of which are using the Internet. Approximately 45% of the world's Internet users are below the age of 25. Over the last 5 years, developing countries have increased their share of the world's total number of Internet users from 44% in 2006, to 62% in 2011. Today, Internet users in China represent almost 25% of the world's total Internet users and 37% of the developing countries' Internet users. International Telecommunications Union, "International Communications Technologies Facts and Figures," <http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf> (accessed 20 February 2012).

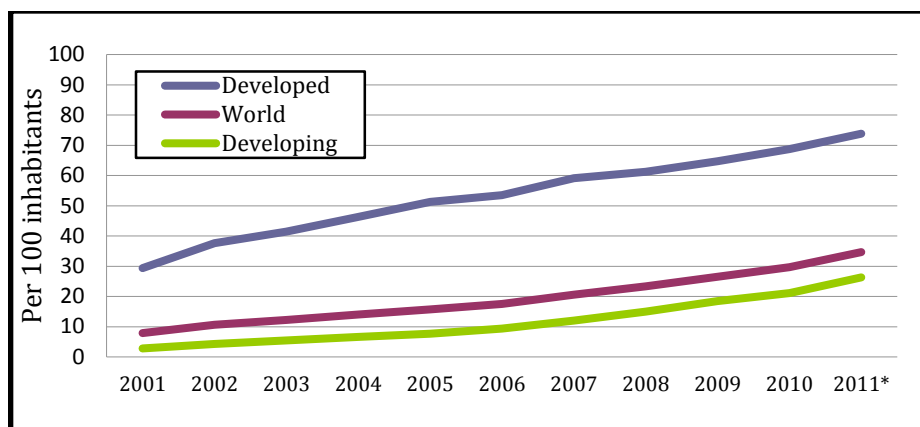


Figure 2: Growth of Internet Users Per 100 Inhabitants
Source: International Telecommunications Union, www.itu.int

The Internet began as a Department of Defense (DOD) research experiment in the 1960s. Its first actualization was named the Advanced Research Projects Agency Network (ARPANET). It was originally constructed to share bundles of electronic information from one system of computers to another. Electronic mail (e-mail) was invented shortly thereafter. This laid the foundation for electronic information sharing. In the 1980s, more networks began showing up because innovations in technology proved to ease the flow of information across geographically separated areas. In 1989, Tim Berners-Lee, at the European Organization for Nuclear Research (CERN) Particle Physics Library, invented what the world now knows as the World Wide Web. Up to this point, the National Science Foundation had limited the use of Internet networks to non-commercial activity. In 1991, this ban was lifted, resulting in an explosion of commercial interest and investment. By 1995, 25 million worldwide users connected to the Internet.⁹

Today, the Internet—specifically the World Wide Web (WWW)—has become the popular visualization of cyberspace. But the scope of the

⁹ This paragraph's information was taken from multiple sources on the history of the Internet. The specific resource was the following: Dennis A. Trinkel and Scott A. Merriman, *The American History Highway—A Guide to Internet Resources on US, Canadian, and Latin American History* (Armonk, NY: M.E. Sharpe, Inc., 2007), 3-5.

Internet, to include the WWW, private networks, and e-mail, goes much further. The key notions of cyberspace are “those of non-linearity, self-organization, and emergence, and the central metaphor is that of the network, the distributed model of information exchange best embodied by the Internet.”¹⁰ Cyberspace goes well beyond just the Internet. Richard Clarke explains in *Cyber War* that: “Cyberspace is all of the computer networks in the world and everything they connect and control,” it “includes the Internet *plus* lots of other networks of computers that are not supposed to be accessible from the Internet.”¹¹ With the networks in cyberspace growing beyond just the Internet, and its nation heavily reliant on cyberspace to run day-to-day life, the DOD found it necessary to define this domain.

Official Definition

In 2003, President George W. Bush’s administration loosely defined cyberspace as the interconnection of hardware (computers, servers, routers, etc.), emphasizing that a healthy cyberspace is essential to the nation’s economy and security.¹² Missing from this definition was an emphasis that cyberspace is an information environment. In 2008, more than 25 years after Gibson coined the term and almost 20 years after the World Wide Web became the face of the Internet, the DOD finally released a memo offering an official definition. Cyberspace is “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”¹³ By defining cyberspace,

¹⁰ Antoine Bousquet, *The Scientific Way of Warfare—Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), 34.

¹¹ Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins Publisher, 2010), 70.

¹² The White House. “The National Strategy to Secure Cyberspace,” February 2003, vii.

¹³ US Office of the Deputy Secretary of Defense, *The Definition of “Cyberspace,”* Policy Memo, 12 May 2009, in DOD, Joint Publication 1-02, *DOD Dictionary of Military and*

the DOD began the long process of attempting to wrap its arms around something that was both familiar and unfamiliar. Information operations (IO) is not a new concept. What is new is the combination of information in a new and unfamiliar environment with tools that are often misused or misunderstood. Cyberspace is unique, and because of this, the DOD has begun to take the steps necessary to gain control of this domain, and use it as an advantage. “The cyberdomain [sic] is unique in that it is human-made, recent, and subject to even more rapid technological changes than other domains.”¹⁴ The military must look for ways to take advantage of these rapid changes. These advantages will be gained through the proper command and control of this environment.

Military Use

Cyberspace includes hardware and software: infrastructure, 1s and 0s, ideas, the Internet, intranets, cellular networks, satellite communications, and military networks such as link-16, blue force tracker, and the secret Internet protocol router network (SIPRNET). Cyberspace, like any other environment in which one can attack and defend, has become something the commander strives to control. The idea of a tightly controlled Internet is popular because “cyberspace provides states and non-state actors the opportunity to negate the United States’ conventional military advantage, circumvent its natural boundaries, and directly attack critical infrastructure.”¹⁵ One must remember that complexity in war existed before cyberspace, but cyberspace has accelerated and amplified these complexities. The effectual strategist *must* understand the enormous scope and complexity of cyberspace and how others—especially policy makers—see cyberspace.

Associated Terms, (8 November 2010), 86.

¹⁴ Joseph S. Nye Jr., *The Future of Power* (Philadelphia, PA: Perseus Books Group, 2011), 124.

¹⁵ Evgeny Morozov. *The Net Delusion—The Dark Side of Internet Freedom* (Philadelphia, PA: PublicAffairs, 2011), 222.

A significant problem with the military's use of cyberspace is the longstanding pursuit of dominance of domains. The ability to ensure one's freedom of action and deny another's is a difficult task. Cyberspace, in its immense scope and complexity, may not be a domain that can be controlled in the traditional sense. Also, there is no physical equivalent to the Internet or cyberspace, and attempting to apply traditional warfare techniques and strategies to cyberspace may not lead to any productive conclusions.¹⁶ The complexity and uniqueness of cyberspace requires an acute understanding to command and control cyber forces and capabilities in order to gain cyber power.

Cyber Power

All your base are belong to us

—Popular Internet Meme, *Zero Wing*

This broken English translation comes from the 1991 Sega videogame, *Zero Wing*, and has since become an Internet meme and part of popular cyber culture.¹⁷ Cyberspace is unique, and so are those things required to gain power its power. Cyber power requires two things: cyber resources and the knowledge to effectively use them. Cyber power is “the national ability to disrupt [the target] somewhere in the digitized globe . . . in proportion to its motivations/capabilities to attack with violent effects and yet be resilient against imposed or enhanced nasty surprises across all critical nationally sustaining systems.”¹⁸ Simply put, cyber power is the ability to attack an enemy

¹⁶ Richard Stiennon, *Surviving Cyber War* (Lanham, MD: Government Institutes, 2010), 48.

¹⁷ Knowing this quote and its origins will undoubtedly provide a strategist with “cyber street cred.” http://en.wikipedia.org/wiki/All_your_base_are_belong_to_us (accessed 5 January 2012).

¹⁸ Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, GA: University of Georgia Press, 2011), ix.

and defend oneself from attack, but achieving this power is a complex and difficult process, especially for the military.

The cyberspace domain is unique, but it is not different enough to change the nature of war. Throughout history, weapons of war have changed more quickly than tactics or the ability of commanders to adapt new strategies. A generation of commanders is now at risk of failing to understand the utility of cyberspace—just as commanders misunderstood the utility of the machine gun in the trenches of the western front and the airplane in the jungles of Indochina. While providing commanders with information at greater speeds than ever before, cyberspace also provides a new environment in which to attack and defend.

Cyberspace can provide two unique opportunities to the warfighter—it can enable warfighting processes or can be used as a weapon. As an enabler, cyberspace is the carrier and provider of information critical to everyday life, mission planning, and the decision making process during war. As a weapon, cyberspace can provide both soft and hard power. In soft power operations, cyberspace is the vehicle that one can use as the foundation of information operations. In hard power operations, network attack and network defense can disrupt an enemy and protect the links critical to the friendly decision making process. These opportunities must be commanded and controlled properly in order for the commander to take advantage of cyberspace's unique attributes.

Information

Cyber is a tool—a vehicle that provides a commander with information. Yet, the commander must control this information and make sound strategic decisions from his interpretation of the incoming data. This “combination of growing dependence and ever-shaky confidence in our control over information systems has given rise...to a

new type of threat . . . information warfare.”¹⁹ This is no new military art—both Carl von Clausewitz and Sun Tzu were acutely aware of the importance of information. Clausewitz was skeptical of its accuracy—believing most intelligence to be false. Sun Tzu emphasized knowing one’s enemy *and* one’s self. The role of information in war has not changed since individuals began writing about war, and cyberspace has neither changed that fact, nor made things any easier. In fact, the US military learned this lesson in its most recent war with Iraq. Although the US was facing a foe mistakenly perceived to be handicapped by a lack of technology, the insurgency in Iraq was more networked, more decentralized, and operated within a wider commander’s intent than any enemy in modern times.²⁰ Accurate and timely information remain one of the most important pieces to the strategic puzzle; unfortunately, cyber has yet to provide better intelligence to the commander, only more of it and at a faster rate. Without authority outside the .mil realm, commanders have little choice but to control what they own and work within the system they do not.²¹

The military leader cannot allow cyber to overwhelm their command. Knowledge and information are “becoming the central resource” in society and the battlespace.²² Because cyber has become a highly demanded and depended upon resource it will most certainly be an integral piece to future strategic puzzles. Wars in the future “will increasingly be prevented, won or lost based on information superiority and dominance.”²³ No one facet in itself is sufficient to guarantee the

¹⁹ Martin C. Libicki, *Conquest in Cyberspace—National Security and Information Warfare* (New York: Cambridge University Press, 2007), 15.

²⁰ Bousquet, *The Scientific Way of Warfare*, 1.

²¹ These specific authority issues will be identified in the second chapter, *Cyber Organization*, with solutions given in the third and fourth chapters.

²² David J. Lonsdale, *The Nature of War in the Information Age* (London: Frank Cass, 2004), 3.

²³ Lonsdale, *The Nature of War in the Information Age*, 51.

successful conduct of command in war—let alone cyber.²⁴ Cyber does not provide magic capabilities. Modern technologies do not provide commanders with a greater ability to command. Technology provides a commander with more information in a faster manner than ever before, and while this information can be the basis for a commander's decisions it can just as easily add to the fog of war.

Command and control (C2) is “the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.”²⁵ Efficient and effective C2 of cyberspace, while difficult, can provide a commander with an ability to integrate forces by ensuring a clear picture of current positions and logistical requirements. The “integration of armed forces into a coherent system maintained by information and communication technologies amenable to centralized control has been an observable trend in all modern industrial armies.”²⁶ This information is critical to a commander due to the changing context of war: “As the range and specialization of military personnel and equipment increase along with the concomitant logistical challenges characteristic of industrial warfare, reliable channels of communication become essential.”²⁷

In a quest for certainty and predictability, since the invention of the telegraph, military commanders have put their faith in the electronic transfer of information. Unfortunately, information is imperfect and warfare cannot be completely controlled, but cyber allows for redundancy that can provide “great adaptability and resilience in the face of contingency.”²⁸ While cyber provides the commander with a certain

²⁴ Martin Van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), 261.

²⁵ *Department Of Defense Dictionary of Military and Associated Terms* (Government Printing Office, Joint Pub 1-02 DOD, 12 April 2001; as amended through August 2005), 59.

²⁶ Bousquet, *The Scientific Way of Warfare*, 130.

²⁷ Bousquet, *The Scientific Way of Warfare*, 130.

²⁸ Bousquet, *The Scientific Way of Warfare*, 218.

vantage point, “the imposing array of electronic gadgetry at their disposal,” provides “no evidence whatsoever of being one whit more capable of dealing with the information needed for the command process than were their predecessors a century or even a millennium ago.”²⁹ More and faster does not change the fact that processing is still required, and commanders must still decide between what information is reliable, important, and true. Decentralization remains a tried and true method of command to help process the overwhelming amount of information cyberspace provides. Decentralization distributes uncertainty throughout the organization and to the lowest level. Commanders must not let the promises of cyberspace tempt them into believing “the notion that technology-driven centralization and fusion of information can overcome uncertainty and decisively impose order and chaos.”³⁰

Cyber War

*You can't say that civilization don't advance . . .
for in every war they kill you in a new way.*

—Will Rogers, 1929

Innovations in technology have historically sparked both interest and fear in the American public. As early as 30 years ago, striking images of cyber war greeted the American public in popular movies and magazines. In 1983, Hollywood portrayed a computer that almost started World War III because it confused a game with the reality of the Cold War.³¹ In August 1985, Time Magazine ran a cover story titled, “Cyber War” with the tagline, “The US rushes to turn computers into tomorrow’s weapons of destruction. But how vulnerable is the home

²⁹ Van Creveld, *Command in War*, 265.

³⁰ Bousquet, *The Scientific Way of Warfare*, 233.

³¹ Internet Movie Database (IMDB), *WarGames*. <http://www.imdb.com/title/tt0086567/> (accessed 15 January 2012).

front?”³² Today, authors like Richard Clarke take advantage of human emotion and warn about doomsday scenarios that are guaranteed by society’s over reliance upon cyberspace and failure to protect against cyber threats. Clarke proclaims that, “Cyber war is real, it happens at the speed of light, it is global, it can skip the battlefield, and it has already begun.”³³ But before one reacts to this exclamation, one must take it at face value, and explore what cyber war truly is and what it entails.



Figure 3: Cyber War

Source: Time Cover Store, 21 August 1995

Cyber war is *not* coming, at least not in this sense. Cyberspace does matter, “but we simply don’t know how it matters,” and this fact “only makes it matter even more: The costs of getting it wrong are tremendous.”³⁴ There will be conflict in cyberspace, and cyber will enable the warfighter, but war in cyber is not the “dripping death” that

³² Time Magazine Cover Store. <http://www.timecoverstore.com/product/cyber-war-1995-08-21/> (accessed 15 January 2012).

³³ Clarke, *Cyber War*, 30-31.

³⁴ Morozov, *The Net Delusion*, 30.

Wells envisioned and Richard Clarke proclaimed for the cyber age.³⁵ Actual conflicts in cyberspace currently resemble vandalism, theft, espionage, and voyeurism—not war just yet. The examples of cyber attack in Estonia and Georgia, and the Stuxnet computer worm in Iran have helped build the exaggerated rhetoric of cyber war, but fortunately the situation is simply not war. Bothering someone in cyberspace is easy—such as defacing a website or overwhelming a server, but this effect is only temporary. Actual damage to a system is not easy—there is a “big difference between disabling a system temporarily and doing so for any great length of time,” and “all this limits the kind of damage that even successful computer network attacks can have.”³⁶ Attack and defense in cyberspace is a complex strategic problem, and control of the forces that attack and defend is integral to sound military strategy.

Cyber war involves offensive and defensive action in the cyberspace domain. These actions are used in an effort to protect one’s own network and “penetrate another nation’s computers or networks for the purposes of causing damage or disruption.”³⁷ These actions are defined by who is taking them. In this case, state actors or governments are the ones taking action against another nation. War in cyber goes beyond just kinetic operations to destroy an enemy’s capabilities. Cyber operations include “the unauthorized penetration by, or on behalf of, or in support of, a government into another nation’s computer system, in which the purpose is to add, alter, or falsify data, or cause the disruption of or damage to a computer, or network device, or the objects a computer system controls.”³⁸ But all actions in cyberspace are not akin to a state-on-state definition of war. While many of these actions are low-threat or

³⁵ Wells envisions war coming from the air with bombs that drop while people sleep, the aircraft “dripping death.” Wells, *War in the Air*, 188.

³⁶ Libicki, *Conquest in Cyberspace*, 37.

³⁷ Clarke, *Cyber War*, 6.

³⁸ Clarke, *Cyber War*, 228.

criminal types of behavior they still must be addressed if one is to maintain a network and have freedom of action in cyberspace.

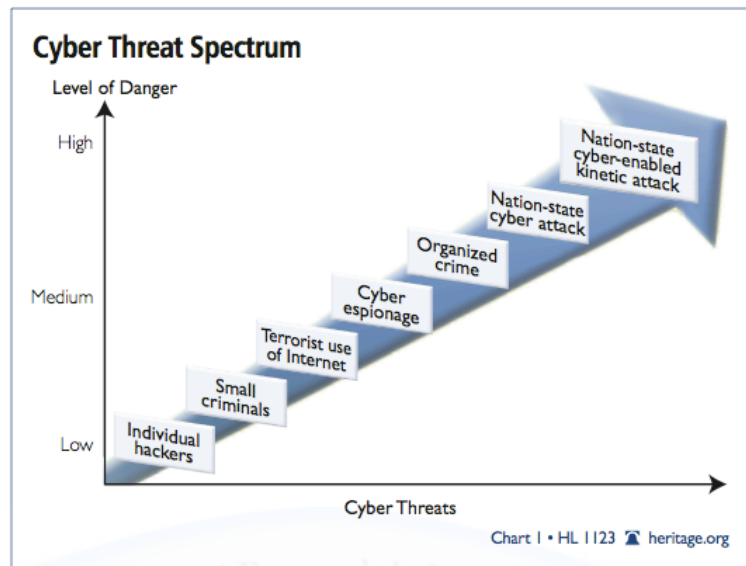


Figure 4: Level of Danger from Cyber Threats

Source: Steven Bucci from the Heritage Foundation's "Heritage Lectures"

Cyber Attack

This paper defines attacks in cyberspace as those actions that involve physical manipulation or exploitation beyond one's own network. Cyber attack can come in two different forms: one against data, the other on control systems. This definition is different than many popular explanations that separate exploitation from attack. Specifically, Martin Libicki separates the two because exploitation "does not deprive the user of the full use of the machine," and "the user suffers no consequential harm other than having secrets stolen."³⁹ This paper groups exploitation and attack together because exploitation could easily turn into manipulation or an adversary could perceive exploitation as an actual attack. The nature of both these intrusions requires the centralized C2 of these capabilities.

³⁹ Martin Libicki, *Cyberdeterrence and Cyberwar*, (Santa Monica, CA: RAND Corporation, 2009), 23.

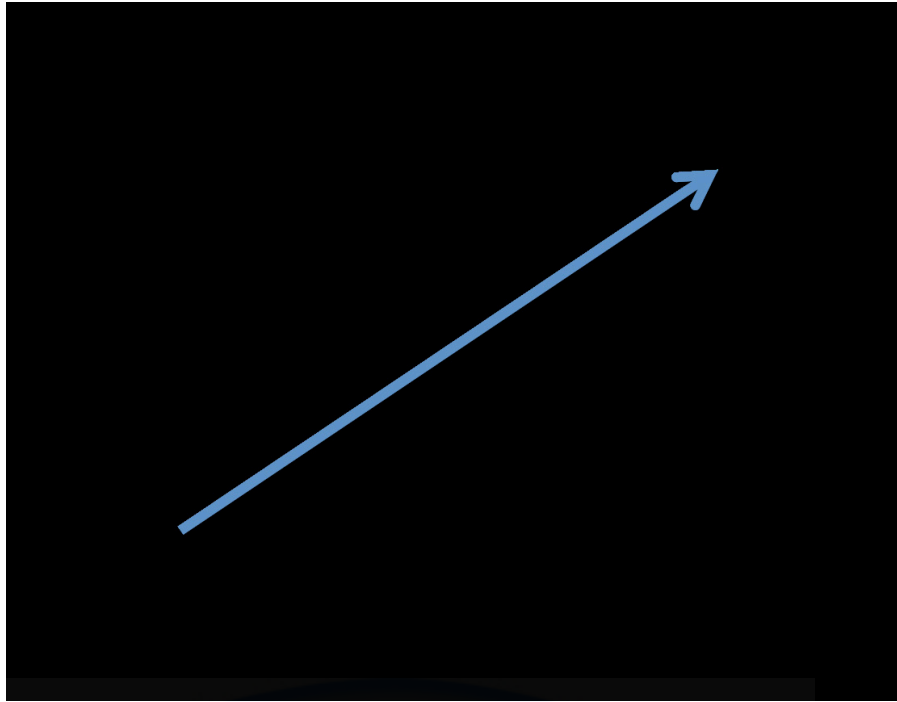


Figure 5: Levels of Cyber Power

Source: Author's Original Work

The first type of cyber attack involves the theft or manipulation of data or the denial of network services. The vast majority of all Internet attacks falls under this category and includes thefts of personal data and credit-card numbers, website vandalism, or a major denial-of-service assault.⁴⁰ The second type of cyber attack involves an assault or attempted take-over of control systems. These systems maintain the operations of physical infrastructure, such as distributed control systems that regulate water, electrical, and railroad networks. While remote access to many control systems have previously required an attacker to dial-in with a modem, these operations are increasingly reliant on the Internet to transmit data or are connected to a company's local network that is itself connected to the Internet.⁴¹

⁴⁰ Robert Murrill, "The Question of Cyber Terrorism," <http://articles.forensicfocus.com/2011/07/23/the-question-of-cyber-terrorism/> (accessed 20 February 2012).

⁴¹ Murrill, "The Question of Cyber Terrorism," (accessed 20 February 2012).

The first form, an attack against data is often perceived to have little ability to cause physical damage or deaths, but can have significant second-order consequences. Although defined as an attack, not all action of this kind alters or damages the actual information being attacked. These actions are akin to espionage. Spying in cyberspace, “to collect information, does not add or alter data, nor does it need to damage or disrupt the network or things that the network controls in physical space, if it’s done well.”⁴²

The second form, against control systems, can result in kinetic actions or damage. This involves turning a system off or altering a system’s actions. These control systems remain vulnerable because they are connected to the Internet and they use system software common in industry. Many power and utility companies “are operated with networks of computer-controlled devices, known as supervisory control and data acquisition (SCADA) systems,” that “could be attacked by overloading a system that, upon failure, causes other operations to malfunction as well.”⁴³ The fact that these companies are often privately owned compounds this vulnerability.

Joint Publication 3-13, *Information Operations*, defines the military’s official employment of cyber attack, or as it is named in this document, network warfare: “The employment of Computer Network Operations (CNO) with the intent of denying adversaries the effective use of their computers, information systems, and networks, while ensuring the effective use of our own computers, information systems, and networks. These operations include Computer Network Attack (CNA), Computer Network Exploitation (CNE), and Computer Network Defense (CND).”⁴⁴ While these definitions are fine, they do little to provide

⁴² Clarke, *Cyber War*, 228.

⁴³ Murrill, “The Question of Cyber Terrorism,” (accessed 20 February 2012).

⁴⁴ Joint Publication 3-13, *Joint Doctrine for Information Operations* (9 October 1998), in Jeffrey Carr, *Inside Cyber Warfare*, 176.

parallels from the nature of cyber to the nature of war—a significant understanding required to properly command in this domain.

The Nature of War With Cyber

Cyberspace, more particularly the Internet, is still the “wild, wild West,” a fact that does not sit well with military commanders who are traditionally taught from the beginning of their careers that power and success stem from the ability to control and command those things in their area of operations. For this reason many from within the US government and military would like to build electronic borders and network castle walls. This is an attempt to manipulate the cyber domain into a more familiar environment, regardless of whether or not that is actually possible or even beneficial. In theory, this should allow them the ability to regulate and control cyberspace but in reality, it must only be used to protect their own networks. The character of war has changed, but its nature has not. Success in war still requires those characteristics shown to us by military geniuses in times past. “No single communications or data processing technology, no single system of organization, no single procedure or method, is in itself sufficient to guarantee the successful or even adequate conduct of command in war.”⁴⁵ Cyberspace is unique, but not in its complexity—the nature of war and the nature of war in cyberspace are not that different.

To explain the nature of war, Clausewitz emphasized the ideas of violence and destruction, uncertainty and chance—the fog and friction of war. Cyber can certainly be an advantage to the commander, but “future force structure, doctrine, strategy and general preparation for war should reflect the nature of warfare, not some idealized vision of the potential offered” by new technologies.⁴⁶ Complex variables and vulnerabilities in war existed long before cyberspace, the Internet just sped up the existing

⁴⁵ Van Creveld, *Command in War*, 261.

⁴⁶ Lonsdale, *The Nature of War in the Information Age*, 95.

system. “Circumstances vary so enormously in war, and are so indefinable, that a vast array of factors has to be appreciated—mostly in the light of probabilities alone.”⁴⁷ Victory in war will go to commanders who better understand the nature of war, who are able to apply proper C2 of offensive and defensive cyberspace measures, and who do not allow cyberspace to narrow their thinking.

Superior organization and strategy are as important to commanders today as they were to Napoleon Bonaparte in the early 19th century. After all, Napoleon’s strategies were revolutionary “in that he possessed the daring and ingenuity needed to transcend the limits that technology had imposed on commanders for thousands of years.”⁴⁸ Napoleon was a military genius, Clausewitz attempted to capture that genius, and cyber has not changed this fundamental fact. Napoleon understood what he could accomplish with the means available to him: “to know what one cannot do, and refrain from trying; and distinguish between the two—that, after all, is the very definition of military greatness, as it is of human genius in general.”⁴⁹ The cyber genius must duplicate this thinking. Commanders must ensure cyber-forces are familiar with cyber issues, and trained for emergencies and attacks. The cyber strategist must be prepared to dynamically innovate according to the changes in technology and adaptation of the threat; and have an offensive plan to attack. The commander who understands the following will gain the advantages of cyberspace: conflict *will* occur in cyberspace and this does *not change* the nature of war.

⁴⁷ Bousquet, *The Scientific Way of Warfare*, 201.

⁴⁸ Van Creveld, *Command in War*, 101.

⁴⁹ Van Creveld, *Command in War*, 102.

Cyber Strategy

But why did they start the War? They couldn't stop themselves. 'Aving them airships made 'em.

—H.G. Wells, *The War in the Air*

“Aving” cyber must not poison the strategist’s mind. Decision makers must not become overzealous with cyber’s offerings. At risk are the same faulty assumptions and decisions that strategists made while sitting in the Air Corps Tactical School (ACTS) during the genesis of airpower discussing how revolutionary technology would be utilized in war. Air Force strategists at ACTS rested their ideas about attacking their enemy on assumptions about “the complexity and vulnerability of modern industrial societies, but they would take a particular interest in what they believed to be the inherent weaknesses of interdependent, interlocking national economic systems.”⁵⁰ For the Air Force, these assumptions culminated with strategic bombing during World War II. It can be argued that, in the end, this strategic small-mindedness led to a multitude of strategic problems that followed in Korea and Vietnam. Cyberspace is also providing the Air Force strategists with a new opportunity, just as strategic bombing “promised them greater independence, responsibility, and prestige.”⁵¹ Unfortunately, these same types of assumptions are guiding today’s cyber strategies.

While Clarke’s visions of a cyber Armageddon can be dismissed, his discussions lead to strategic discussions regarding the impact of cyber. “Cyber weapons would have a far lesser impact than nuclear weapons, but their employment under certain circumstances could be highly damaging and could also trigger broader war.”⁵² The problem lies

⁵⁰ Tami Davis Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas About Strategic Bombing, 1914-1945* (Princeton, NJ: Princeton University Press, 2004), 128.

⁵¹ Biddle, *Rhetoric and Reality in Air Warfare*, 129.

⁵² Clarke, *Cyber War*, 211.

in action taken in cyberspace that may have unforeseen consequences elsewhere. If a cyber warrior hacks into a network, even just for purposes of espionage, it is not too far a leap to imagine that action may actually disrupt the data or the system, and in a worst-case scenario actually cause physical damage. Because of the weight and scale of operations in cyberspace, questions remain on the command and authority of these actions: “. . . who gets to decide to use them, and how do we make sure they are not used without authorization? Who should decide what networks we should be penetrating as part of the preparation of the battlefield?”⁵³ Commanders should also anticipate highly restricted rules of engagement (ROE) when it comes to cyber war. In the foreseeable future, much like all historically held strategic weapons, the control of cyber may reside in the hands of the president of the US or the Secretary of Defense.

Cyberspace enables the warfighter just as it has since the advent of electronic communication; however, cyber is a much more powerful metaphor than it is a weapon. Yet, cyber is just a tool. One that can provide incredible speed and large amounts of information to the commander, but it can also prove to be incredibly complex and difficult to implement properly. If used inappropriately, cyber's hurdles can prove more costly than its benefits. Unless strategists understand these complexities, or at the very least accept that this is a complex issue, they will be relegated to using cyberspace with unrealistic ideas and uncreative methods. Military users of cyberspace must not become so small-minded that its implementation becomes the strategic bombing of the next war. Strategic military questions, and on a grander scale, national security questions, must be answered without proclaiming the miraculous wonders of cyberspace. The right answer is that cyber presents an incredibly complex problem that will continue to be at the

⁵³ Clarke, *Cyber War*, 211.

forefront of strategists' minds. Cyberspace may be new, but complexity, information, and ideas are not.

In 2011, the White House released its cyberspace strategy. Concerning hostile acts in cyberspace, the statement emphasizes two things: the right to self-defense, and the reaction to hostile acts in cyberspace will not be limited to that domain:

When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.⁵⁴

Summary

Cyberspace is an operational domain of interconnected electronic networks that consists of infrastructure, software, and ideas. It is an operational environment, “where humans and their organizations use the necessary technologies to act and create effects, whether solely in cyberspace or in and across the other operational domains and elements of power.”⁵⁵ In simpler terms, cyberspace is a networked electronic information environment. The importance of cyberspace is not in question. Cyberspace and the “Internet does matter, but we don’t know how it matters. This fact, paradoxically, only makes it matter even more:

⁵⁴ The White House, “International Strategy for Cyberspace,” (May 2011), 14.

⁵⁵ Daniel T. Kuehl, “Cyberspace to Cyberpower: Defining the Problem”, in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (eds.), *Cyberpower and National Security*, (Dulles, VA: Potomac Books, Inc.: 2009), 29.

The costs of getting it wrong are tremendous.”⁵⁶ Understanding the complexities of this domain and how to use its power to one’s advantage will be a defining characteristic of tomorrow’s military genius.

Joint Publication 3-13, *Joint Doctrine for Information Operations*, defines cyberspace operations as a core capability for joint operations. The importance of cyberspace plans and activities are reinforced by “the increasing reliance of unsophisticated militaries and terrorist groups on computers and computer networks to pass information to C2 [command and control] forces.”⁵⁷ The ease of access into the cyber domain will remain an obstacle for the US military. Joint Pub 3-13 continues, “As the capability of computers and the range of their employment broadens, new vulnerabilities and opportunities will continue to develop. This offers both opportunities to attack and exploit an adversary’s computer system weaknesses and a requirement to identify and protect our own from similar attack or exploitation.”⁵⁸ So, down at sea level, cyberspace is easy and inexpensive to access, opportunities are broadening, but so is the threat. Currently, a cohesive cyber warfare strategy has yet to be defined, and the details of organization, authorities, training, and command are still up in the air. The following chapters will address these matters.

⁵⁶ Morozov, *The Net Delusion*, 30.

⁵⁷ Joint Publication 3-13, *Joint Doctrine for Information Operations* (9 October 1998), II-5.

⁵⁸ JP 3-13, II-5.

Chapter 2

Cyber Organization

USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries

—USCYBERCOM Mission Statement

9ec4c12949a4f31474f299058ce2b22a

—USCYBERCOM Mission Statement
(MD5 message-digest algorithm)

Cyberspace provides immense capabilities *and* vulnerabilities, and getting there is easy. Access to cyberspace is relatively easy because it requires only minimal investment from users. While this access allows for the continued development of cooperation on a global scale, it also allows the negative user—those that would attempt to disrupt and attack others in cyberspace—the same advantages. While the Clausewitzian sense of total cyber war may not be on the horizon, cyber attacks on America’s commercial industries, national infrastructure, and military networks occur on a daily basis. The United States is reliant on its networks, and its military shares this dependence. In order to protect its networks and ensure the continued access to cyberspace, the US military must have well-established capabilities to operate in and command cyberspace. In the early 2000s, the fundamental ideas used to begin this process were set in place.

In 2005, spurred by the escalating numbers of attacks highlighting weaknesses in the Department of Defense’s (DOD’s) networks and their ability to command in this unique domain, the gravity of cyberspace

finally became apparent to the Pentagon. The “Air Force, Navy, and intelligence agencies engaged in a bitter struggle to see who would control this new area of warfare.”¹ In cyberspace, command and control (C2) is specifically divided between cyber attack and the defense of the military’s networks. The preexisting unified command structure organizes cyber power. Unified command brings all the services into a joint and integrated structure; and, after all, “there were already Unified Commands for transportation, strategic nuclear war, and for each of the world’s regions.”² This organizational guidance allows the military command structure to adapt to evolving threats. In the case of cyberspace, these evolving threats have grown large enough to necessitate national security interests.

This chapter explores the military’s organizational reaction to cyberspace and cyber threats in four sections. It begins with *Unified Command* examining the existing command structure of the DOD. The second section, *STRATCOM—Before CYBERCOM*, applies this existing command structure and the implementation of strategic capabilities. Next, in *The Air Force in Cyberspace*, this chapter explores the Air Force’s attempt to gain control of this new domain. The final section, *CYBERCOM*, explains how cyberspace fits into a strategic unified command. In the end, the military must organize its cyber operations and resources to create offensive and defensive C2 advantages in warfare.

¹ Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins Publisher, 2010), 35.

² Clarke, *Cyber War*, 35.

Unified Command

In enacting this Act, it is the intent of the Congress . . . to place clear responsibility on the commanders of the unified and specified combatant commands for the accomplishment of missions assigned to those commands [and] to ensure that the authority of the commanders of the unified and specified combatant commands is fully commensurate with the responsibility of those commanders for the accomplishment of the missions assigned to their commands.

—Goldwater-Nichols Department of Defense Reorganization Act, 1 October 1986

Unified command is a concept that allows commanders to maintain authority over their assets while also supporting the mission of separate or larger commands. The DOD defines unified command as “a command with a broad continuing mission under a single commander and composed of significant assigned components of two or more military departments that is established and so designated by the president, through the Secretary of Defense with the advice and assistance of the Chairman of the Joint Chiefs of Staff.”³ This model is meant to provide avenues where the different services can work together. In 1986, actions were taken to strengthen and unify the separate command authorities and assets of the United States military. *The Goldwater-Nichols Department of Defense Reorganization Act of 1986* provided these joint command authorities to the combatant commanders.⁴ This act also established the chain of command for unified commands that ran from the commander to the Secretary of Defense to the President.

Unified combatant commands have “a broad, continuing mission under a single commander . . . which is composed of forces from two or

³ Joint Pub 1-02, (12 April 2001; as amended through August 2005), in William Carwile, “Unified Command and the State-Federal Response to Hurricane Katrina in Mississippi”, *Homeland Security Affairs* 1, Article 6 (August 2006), 1, <http://www.hsaj.org/?fullarticle=1.2.6> (accessed 15 February 2012).

more military departments.”⁵ There are currently nine unified combatant commanders divided between two responsibilities: geographic and functional. Geographic commands assign responsibilities by specific areas of responsibility, and the functional commands assign responsibilities not bounded by geography. There are six geographic commands: United States Northern Command (USNORTHCOM), United States Africa Command (USAFRICOM), United States Central Command (USCENTCOM), United States European Command (USEUCOM), United States Southern Command (USSOUTHCOM), and United States Pacific Command (USPACOM). The three functional commands are: United States Special Operations Command (USSOCOM), United States Strategic Command (USSRATCOM), and United States Transportation Command (USTRANSCOM). These commands, regardless of geographic or functional responsibility, have at least one thing in common: they rely on cyberspace to facilitate actions and they each have their own networks that require defense.

Military Unified Commands are made up of units that are assigned to the command through a joint document called the Unified Command Plan (UCP). The UCP provides guidance for combatant commanders with the intent of setting objectives for situations where two or more entities have command authorities and assets. It defines the formal C2 relationships between military entities. As an allowance of the UCP, “Representatives of the entities meet to set goals and decide how each can contribute to the achievement of those goals.”⁶ This plan also “establishes combatant command missions, responsibilities, and force structure; delineates geographic areas of responsibility for geographic

⁵ Global Security Website, *Unified Command Plan*, <http://www.globalsecurity.org/military/agency/dod/unified-com.htm> (accessed 20 February 2012).

⁶ Carwile, “Unified Command,” 1.

combatant commanders; and specifies functional responsibilities for functional combatant commanders.”⁷

The command of cyberspace lies within this organizational context. As seen in Chapter 1, *Cyber Primer*, the United States and its military rely heavily upon the cyberspace domain. This domain is unique and includes personnel, assets, and a new concept of the battlefield. It also requires a thorough understanding of where to apply cyberspace to support current strategies, and how build new strategies where cyber is the focus. Without appropriate organization and command relationships, this process will not occur. The following sections will explore the current organizational structures and examine whether or not these are providing the military with the capabilities necessary to plan and conduct strategic operations in cyberspace.

STRATCOM – Before CYBERCOM

The Strategic Air Command will be prepared to conduct long-range offensive operations in any part of the world either independently or in cooperations with land and naval forces . . . to conduct maximum-range reconnaissance over land or sea . . . [and] to provide combat units capable of intense and sustained combat operations employing the latest and most advanced weapons.

—General Carl A. Spaatz
1946 letter to Strategic Air Command

After World War II, the responsibility of atomic energy was taken out of the military’s hands because it was “deemed too important to be left to generals.”⁸ The perceived power of atomic technology had escalated beyond the bounds of a single service, and its strategic

⁷ <http://www.globalsecurity.org/military/agency/dod/unified-com.htm>, (accessed 20 February 2012).

⁸ Walter McDougall, *The Heavens and the Earth: A Political History of the Space Age* (Baltimore, MD: The Johns Hopkins University Press, 1997), 84.

implications were so high that new organizations were deemed necessary for its care. Strategic Air Command (SAC) would deliver the atomic weapons, but the Atomic Energy Commission (AEC) was “empowered to develop and direct the use of [this] specific technology.”⁹ These conditions set the stage for the centralization of command of strategic weapons. Nuclear weapons were unique, and due to their incredible destructive power, and “the speed of the delivery systems (first bombers then intercontinental ballistic missiles), it became crucial to ensure a very tight control over their use, as well as develop effective early warning mechanisms for a credible nuclear deterrent.”¹⁰ Cyber, like its nuclear predecessor, is so unique that it requires centralized command of its attack capabilities. While cyber war is not coming, the implications of cyber actions can still have devastating strategic effects. Actions in cyberspace can be interpreted much differently than what was actually intended. Cyber’s power has escalated beyond the bonds of a single service, and its strategic implications are so high that new organizations have been deemed necessary for its care. STRATCOM, SAC’s successor, seemed like the logical fit.

STRATCOM is currently charged with multiple missions. The unified command is in charge of global strike, space, integrated missile defense, intelligence, surveillance, and reconnaissance (ISR), and cyberspace. STRATCOM was first established in 1992, holding the responsibilities of military nuclear operations. In 2002, the unified command SPACECOM was dissolved and its responsibilities were added to STRATCOM. Today, STRATCOM’s responsibilities include strategic deterrence, global strike, and operating the DOD’s global information grid (GIG).¹¹

⁹ McDougall, *The Heavens and the Earth*, 84.

¹⁰ Antione Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York, NY: Columbia University Press, 2009), 130.

¹¹ STRATCOM Official Website, <http://www.stratcom.mil/history/> (accessed 22 February 2012).

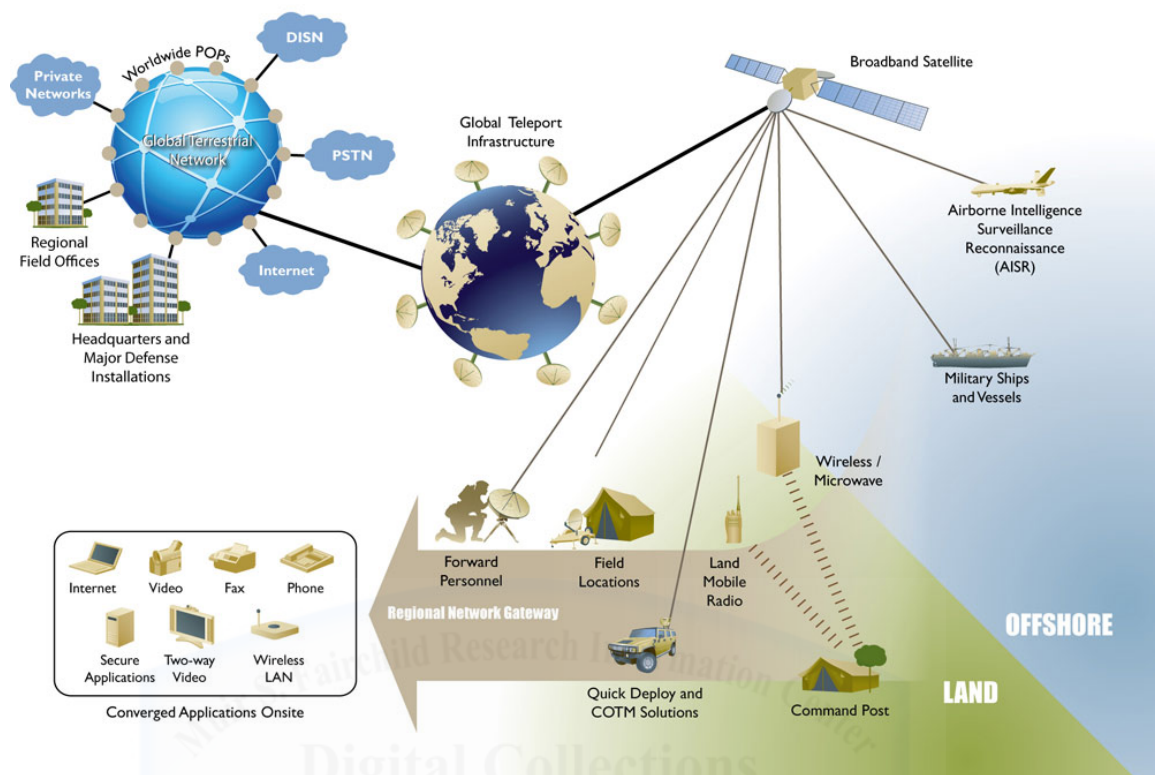


Figure 6: The Global Information Grid

Source: Harris CapRock,

<http://www.harriscaprock.com/government.php#!prettyPhoto>

Before CYBERCOM, the military organized cyberspace-related operations through information operations (IO). Joint Publication 3-13, *Information Operations*, defines the five core capabilities of IO: electronic warfare (EW), computer network operations (CNO), physiological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC). CNO attempted to command cyberspace. CNO is defined as the attempt to “attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure.”¹² These networked computers and information technology (IT) infrastructure systems define the way cyberspace is understood. CNO is divided into

¹² DOD, Joint Publication 3-13, *Information Operations*, II-4 – II-5.

three categories. First, computer network exploitation (CNE) is used to collect intelligence information from and about computer networks. Second, computer network attack (CNA) is used to destroy or disrupt the adversary's ability to use their computer network. Third, computer network defense (CND) is used to protect one's own computer networks. These three categories are necessary in order for the military and its unified commanders to meet and exploit the cyber threat while still defending their networks. CNE and CNA will be further explored in Chapter 4, *Command and Control of Cyber Attack*, and CND will be examined in Chapter 3, *Command and Control of Cyber Security*.

The history of organizing cyberspace into military organization is short and at times difficult to follow. In 1998, Joint Task Force (JTF) CND was created and handed the responsibility of defending the DOD's information grid. Curiously, it was almost three years before attack in cyberspace was included. With this, the JTF was renamed, JTF-CNO. This move brought both offensive and defensive action under a single task force. But given the different natures of cyber attack and cyber defense, separate commands seemed logical choices to assume these separate responsibilities. To some, NORTHCOM seemed like the logical choice to receive responsibility of CND. Defense of networks is "an area critical to homeland defense, which, like national infrastructure, will involve far more DOD efforts," and with "ties to the civil sector, the command may prove best sited to integrate military capabilities and procedures with others to thwart this new age of national security hazard."¹³ Cyber attack, which had already begun to be accepted as highly strategic in nature, was thought best placed in the hands of another command. The decision to attack in cyber, "like strategic nuclear weapons... will probably be made by the President or Secretary of Defense, and plans to employ such weapons should be integrated into

¹³ W. Spencer Johnson, "New Challenges for the Unified Command Plan," *Joint Forces Quarterly*, (Summer 2002), 67.

war plans of regional commands, much like come nuclear weapons.”¹⁴ Following this line of logic, STRATCOM seemed the perfect fit for cyber attack. However, with offense and defense functions separated, there runs the risk of cyberspace operations remaining divided and contested.

In 2002, STRATCOM took responsibility of information operations (IO) for the DOD. This came from a change in the UCP, and “undertook a wide-ranging reorganization that included the creation of several joint task forces (including one for global network operations) and joint functional component commands (including one for network warfare).”¹⁵ JTF-CNO was moved under STRATCOM and renamed JTF-Global Network Operations (JTF-GNO). STRATCOM and JTF-GNO now held the responsibilities of CNE, CNA, and CND. However, offensive attack was removed from the task force with the creation of a new organization Joint Force Component Command-Network Warfare (JFCC-NW). Therefore JTF-GNO was responsible for the care and feeding of DOD networks, and JFCC-NW was responsible for exploitation and attack outside of the military’s networks. These task forces remained until the establishment of CYBERCOM, which was charged to pull “together existing cyberspace resources, creating synergy that did not previously exist and synchronizing war-fighting effects to defend the information security environment.”¹⁶

These moves were made to improve STRATCOM’s “ability to operate in cyberspace and carry out critical missions in support of military and national security strategy.”¹⁷ Unfortunately, this new organization did little to put the structures in place to command

¹⁴ Johnson, “New Challenges for the Unified Command Plan,” 67.

¹⁵ Daniel T. Kuehl, “From Cyberspace to Cyberpower: Defining the Problem,” in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (editors), *Cyberpower and National Security* (Dulles, VA: Potomac Books, Inc., 2009), 35.

¹⁶ The majority of this paragraph’s historical information comes from the history section of STRATCOM’s public website, <http://www.stratcom.mil/history/> (accessed 22 February 2012).

¹⁷ Kuehl, “From Cyberspace to Cyberpower,” in Kramer (et al), *Cyberpower and National Security*, 35.

cyberspace across the spectrum of military operations. At this point in the development and understanding of cyberspace, the command and organization of a new and undefined domain was still up in the air. These were the initial steps the DOD took to incorporate cyberspace into military command. Unfortunately, these early actions separated the two main pillars of cyber power and left the organization and command of cyber separate and disjointed—a far cry from the intent of Goldwater-Nichols and the UCP.

The Air Force in Cyberspace

The mission of the United States Air Force is to deliver sovereign options for the defense of the United States of America and its global interests—to fly and fight in Air, Space, and Cyberspace.

—Official Mission of the United States Air Force

In 2005, the Air Force made an aggressive doctrinal claim that the cyber domain was included in its “fly, fight, and win” mission.¹⁸ With this statement, the Air Force asserted that cyberspace is a warfighting domain, and raised its importance to equal status among air and space. Air Force leadership has shown a progressive attitude towards cyber reflecting a “strong desire to play the leading role for the US in cyber war.”¹⁹ In fact, the Air Force was the first service to create an organization for the purpose of exploiting and fighting in the cyber domain: US Air Force Cyber Command (AFCYBER). This was the first service-significant organizational change made in response to cyberspace in the DOD. AFCYBER’s mission was “to prepare for fighting wars in cyberspace by defending national computer networks, running critical

¹⁸ Air Force Public Website, <http://airforce.com/learn-about/our-mission/> (accessed 19 January 2012).

¹⁹ Clarke, *Cyber War*, 34.

operations, and attacking adversary computer networks.”²⁰ The establishment of an operational command for cyberspace would enable the Air Force to employ “global cyber power across the full spectrum of conflict.”²¹ Cyber power would allow the Air Force to look for, find, engage, and act upon its cyber adversaries.

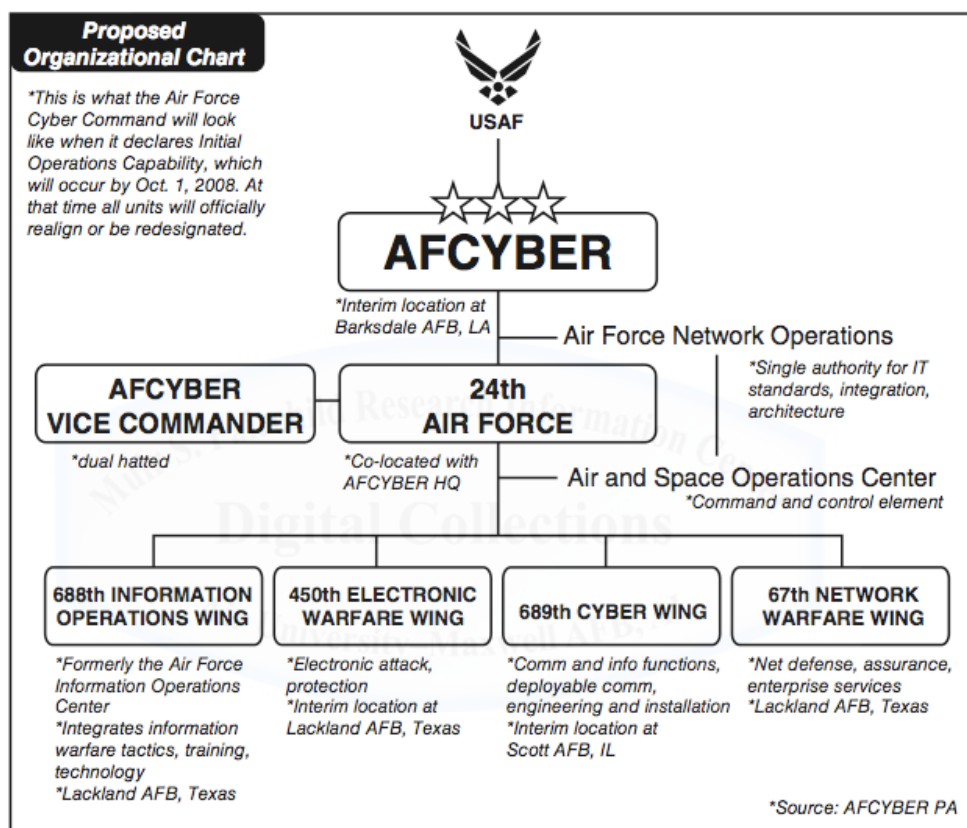


Figure 7: AFCYBER Proposed Organizational Chart
Source: AFCYBER Public Affairs

By establishing a new command, the Air Force began the steps necessary to include cyberspace in the programs and budget plans to organize, train, and equip the Air Force into a cyber fighting force. AFCYBER was given a strategic vision that included the goal of

²⁰ Elihu Zimet and Charles L. Barry, “Military Service Overview,” in Kramer (et al.), *Cyberpower and National Security*, 301.

²¹ Kuehl, “From Cyberspace to Cyberpower,” in Kramer (et al.), *Cyberpower and National Security*, 34.

“dominating cyberspace,” in order to “establish, control, and use” the domain.²² Major General William T. Lord, then commander of AFCYBER, explained that this new command would develop a new type of warfighter: “We will harness this intellectual capital and focus on developing a new form of orientation known as ‘cyber-mindedness.’ Similar to the concept of ‘air-mindedness’ already imbued into every Airman, cyber-mindedness involves the unhindered development of cyberspace capabilities to achieve desired effects.”²³

Major General Lord, in his 2008 article “USAF Cyberspace Command: to Fly and Fight in Cyberspace,” concluded that harnessing cyber technology and personnel capable of operating within this new domain offered the Air Force with a brand new Airman with “cyber-mindedness.” This was not only a new identity, but also an identity that required an institutional change. This mindset involves the unhindered development of cyber capabilities to achieve desired effects.²⁴ The new cyber identity promised to continue to enable and enhance the Air Force’s warfighting capability. General Lord continued that AFCYBER, as of 2008, had already evolved by integrating with air and space in ways our fathers could never have imagined.²⁵ General Lord believed that effective C2 of AFCYBER capabilities would preserve the heritage and traditional role of the Air Force as America’s first choice for achieving strategic, operational, and tactical effects, ultimately preserving

²² Air Force Secretary Michael Wynne and Air Force Chief of Staff General T. Michael Moseley laid out the Air Force’s new vision for cyberspace in a 2006 memorandum entitled “Establishment of an Operational Command for Cyberspace,” in Kuehl, “Cyberspace to Cyberpower,” in Kramer (et al), *Cyberpower and National Security*, 34.

²³ William T. Lord, Major General, USAF, “USAF Cyberspace Command: To Fly and Fight in Cyberspace,” *Strategic Studies Quarterly* (Fall 2008), 14.

²⁴ Lord, “USAF Cyberspace Command,” 14.

²⁵ Lord, “USAF Cyberspace Command,” 16.

America's security for the future.²⁶ In 2008, before AFCYBER had reached operational capability, the command was officially halted.²⁷

In 2009, the Air Force Posture Statement—the document that defines the focus of the Air Force's strategy to fulfill its role in national defense—included for the first time “Cyberspace Superiority” as one of the twelve Air Force core functions.²⁸ One year later, the Air Force began the personnel transition to organize a cyber force. Approximately 3,000 officers saw their job titles change from 33S communications officers to 17D cyber operations officers, and their badges transform to cyber-wings. A senior Air Force general highlighted the significance of this change: “The Air Force mission—to fly, fight and win in air, space and cyberspace—acknowledges the significance and interrelationship of our three operational domains in effective warfighting. The establishment of the Air Force cyberspace badge underscores the crucial operational nature of the cyberspace mission.”²⁹ Once again, the Air Force was making every attempt to become the DOD's cyber experts.

However, after CYBERCOM was established, the Air Force was no longer able to keep its cyberspace command. With that, AFCYBER transformed to a numbered air force, the 24th Air Force (24AF). Its mission is to “provide combatant commanders with trained and ready cyber forces to plan and conduct cyberspace operations, and to extend, maintain and defend the Air Force portion of the global information grid.”³⁰ These actions were an attempt by the Air Force to gain control of

²⁶ Lord, “USAF Cyberspace Command,” 16.

²⁷ This action was taken after Air Force Secretary Wynne and Chief of Staff of the Air Force General Moseley were fired by Secretary of Defense Gates, and General Norton Swartz was named the new Air Force Chief of Staff.

²⁸ Headquarters Air Force, “United States Air Force Posture Statement” (Fiscal Year 2010), 3.

²⁹ Michael Basla, Major General, USAF, AFSPACE vice commander, “New Air Force cyberspace badge guidelines release,” *Air Force Official Website*, 27 April 2010, <http://www.af.mil/news/story.asp?id=123201885> (accessed 18 January 2012).

³⁰ 24AF Official Website, <http://www.24af.af.mil/library/factsheets/factsheet.asp?id=15663> (accessed 1 April 2010).

the opportunities in cyberspace. Not only was this service attempting to command and control this new and unique domain, the Air Force was attempting to build forces with the mindsets necessary to properly manage this domain along with its amplifications and accelerations.

The Five Assertions of Cyberspace

By adding cyberspace to its fly, fight, and win mission, the Air Force has put cyberspace on even ground with the air and space domains. The Air Force “considers cyberspace superiority an imperative and establishes the proposition that it is the prerequisite to effective US military operations in all other warfighting domains.”³¹ The Air Force has laid out its beliefs about the cyberspace domain by asserting the following:

1. The intelligence collector and the information service provider should be separate organizational functions and not dual-hatted.
2. The domain of cyberspace goes well beyond the Internet. The Air Force considers cyberspace a physical domain, through interlinking by the electromagnetic spectrum and electronic systems, rather than a virtual domain.
3. The battle to achieve cyber superiority in any conflict must be fought in a distributed network rather than from one location where there may be a central coordinating element.
4. The control of cyber weapons effects are controllable and the targeting and collateral damage issues are no different than with effects created by explosive or kinetically destructive means.
5. Defense of the cyberspace domain requires a holistic network approach rather than just increased security at each individual node.³²

³¹ Zimet (et al.), “Military Service Overview,” in Kramer (et al.), *Cyberpower and National Security*, 300.

³² Zimet (et al.), “Military Service Overview,” in Kramer (et al.), *Cyberpower and National Security*, 300.

CYBERCOM

The Department of Defense requires a command that possesses the required technical capability and remains focused on the integration of cyberspace operations. Further, this command must be capable of synchronizing warfighting effects across the global security environment.³³

—Secretary of Defense Robert Gates
Memorandum Establishing CYBERCOM,
2009

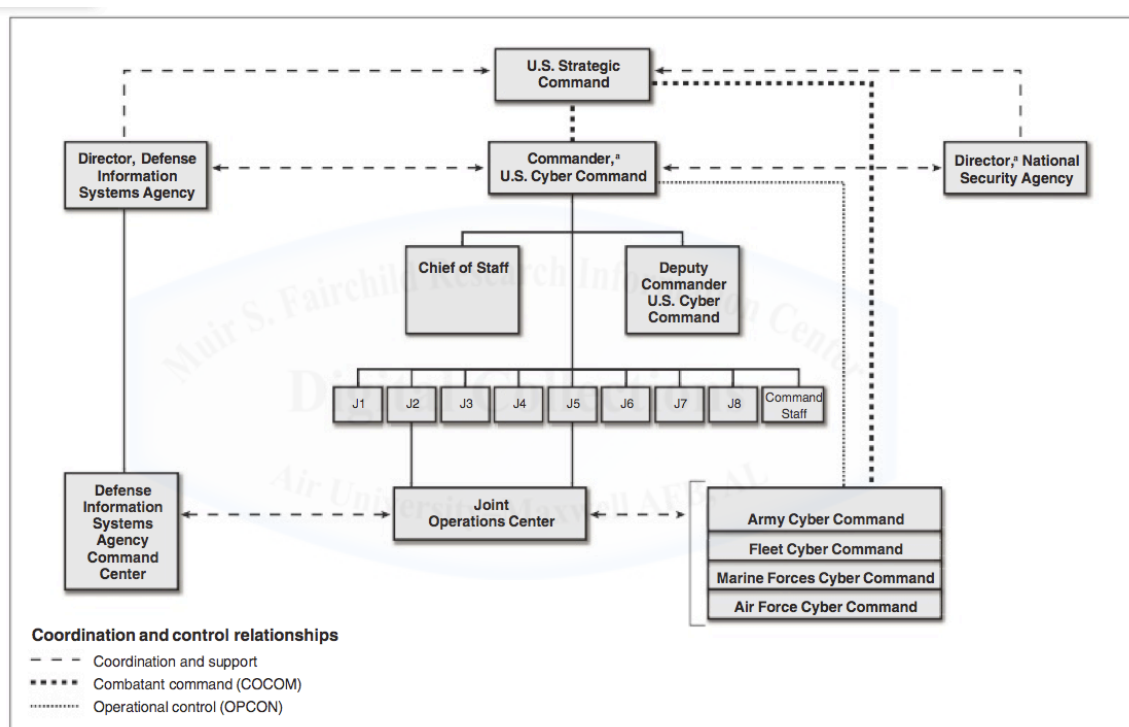


Figure 8: USCYBERCOM Organizational Chart

Source: Government Accountability Office Report to Congressional Requestors—Defense Department Cyber Efforts, May 2011

³³ Secretary of Defense, “Memorandum from the Secretary of Defense: Establishment of a Subordinate Unified US Cyber Command Under US Strategic Command for Military Cyberspace Operations,” *Wall Street Journal*, 23 June 2009, <http://online.wsj.com/public/resources/documents/OSD05914.pdf> (accessed 19 March 2012).

In 2009, the DOD established United States Cyber Command as a subordinate unified command under STRATCOM. CYBERCOM was established to protect the “dot-mil.” With the responsibility of the DOD’s networks came the recombining of the offensive and defensive pillars of cyberspace. CYBERCOM is charged to pull “together existing cyberspace resources, creating synergy that did not previously exist and synchronizing war-fighting effects to defend the information security environment.”³⁴

The establishment of CYBERCOM was in response to an attack on the military’s classified computer networks that identified a significant weakness in the DOD: an inability to organizationally defend critical networks and a lack of authority to act in those networks. Since the Pentagon first connected its networks to the Internet in 1995, its electronic infrastructure and networked systems have been riddled with attack. After a significant attack, the defense and subsequent clean up of the DOD’s unclassified but sensitive Internet protocol router network (NIPRNET) cost over \$100 million in just six months.³⁵ This large amount of investment points not only to the importance of which the DOD holds its networks, but also the number of attacks it was absorbing. The NIPRNET was not the only network found to be vulnerable to attack. In 2008, the secure Internet protocol router network (SIPRNET), the DOD’s classified version of the Internet was infiltrated by a logic worm that found its way in via a common universal serial bus (USB) thumb drive. After years of attacks, the military was finally awoken to its vulnerability to cyber attacks. This response transformed the DOD’s approach to cyberspace. It galvanized “the creation of a new military command charged with bolstering the military’s computer defenses and preparing for eventual offensive operations,” and also “demonstrated the

³⁴ STRATCOM’s public website, <http://www.stratcom.mil/history/> (accessed 22 February 2012).

³⁵ Richard Stiennon, *Surviving Cyber War* (Lanham, MD: Government Institutes, 2010), 48.

importance of computer espionage in devising effective responses to cyberthreats.”³⁶

The decision to make CYBERCOM a sub-unified command was made in part to ensure that the DOD was not over reacting to the new cyberspace domain. This overreaction happened with Space Command (USSPACECOM). In 1985, SPACECOM became a unified command with the promise that the military could gain control of the space domain. By the early 2000s, it had become apparent that the military was not going to have a larger role in space, and the space domain would remain outside of the war-fighting realm. SPACECOM “lasted from 1985 to 2002, by which time it had become clear that neither the US nor any other government had the money to do much in space,” and SPACECOM “was folded into STRATCOM, which operates the strategic nuclear forces.”³⁷

CYBERCOM’s mission is to defend the DOD’s cyber environment through CNO. It is important to understand that this mission does not include civilian institutions or infrastructure, which is the mission of the Department of Homeland Security (DOHS).³⁸ The DOHS’s responsibility entails protecting the infrastructure and cyberspace that not only makes most of America function, but most of its military as well. Cyberspace’s environment is complex and unique in that the military relies heavily on the public sector and non-DOD institutions for control and protection. These will most certainly be issues highlighted in the yet to be written policies in which the public, private, and military sectors of the US will fight for authorities. For the military strategist, cyberspace is a complex operational environment where weapons, policies, functions, and authorities continue to evolve. So, while “Cyber Command may have the

³⁶ Ellen Nakashima, “Cyber-intruder Sparks Massive Federal Response—and Debate over Dealing with Threats”, *Washington Post*, 8 December 2011, http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html (accessed 14 December 2011).

³⁷ Clarke, *Cyber War*, 35.

³⁸ Clarke, *Cyber War*, 43.

resources to help against an attack against the US energy grid,” it is “prevented by law/policy from helping.”³⁹ CYBERCOM, the DOHS, and American civilian institutions must address these issues.

CYBERCOM Authorities

CYBERCOM’s cyberspace authorities and responsibilities have yet to be spelled out in official doctrine. However, Joint Publication (JP) 3-13, *Information Operations*, which includes CNO, does detail the relationship between the STRATCOM commander (CDRUSSTRATCOM) and other combatant commanders. CYBERCOM falls under the command of STRATCOM, but that does not diminish the fact that cyberspace operations may fall simultaneously under specific areas of responsibility (AOR) and across functional boundaries. JP 3-13 explains this relationship for IO, and cyberspace operations fall under this umbrella. It is imperative that combatant commanders “coordinate, integrate, plan, execute, and employ IO,” or in this case CNO within their AOR.⁴⁰ These efforts are directed at achieving the commander’s specific objectives, such as “shaping the operational environment for potential employment during periods of heightened tensions, or in support of specific military operations.”⁴¹ In these cases STRATCOM will be supporting the combatant commander. But, as discussed in Chapter 1, the domain of cyberspace is not limited to just a single AOR. The combatant commander may find that while being supported by STRATCOM it is also necessary to be in a supporting role as well. Due to the characteristics of the cyber domain, cyberspace responsibilities of STRATCOM and combatant commanders will lie across multiple theater boundaries.

³⁹ Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Waltham, MA: Syngress, 2011), 215.

⁴⁰ JP 3-13, *Information Operations*, IV-2.

⁴¹ JP 3-13, *Information Operations*, IV-2.

The National Security Agency

JP 3-13 also details the support the NSA can provide the combatant commander: “NSA support for IO may be coordinated through the J-2 representative of the IO cell or directly with a NSA representative,” and includes the following:

1. Information security technology, products, and services.
2. Vulnerability and threat analyses to support IA and the defense of US and friendly information systems.
3. Determining exploitation risk for telecommunications systems.
4. Determining releasability [sic] of COMSEC materials to allies or coalition partners.
5. Providing technical expertise for CNO.⁴²

Civil Operations

American people, telecommunications, electricity grid, water, and banking infrastructure are all vulnerable to some level of cyber attack. But the Internet and its infrastructure assets are beyond the authority of the government. This makes power, control, and security in cyberspace difficult to visualize. The DOHS defends the non-military portions of government networks. This means there is no governmental entity in charge of protecting America’s corporations and institutions critical to everyday life. It bears repeating, “There is *no* federal agency that has the mission to defend the banking system, the transportation networks, or the power grid from cyber attack.”⁴³ While this issue is beyond the purview of this paper, strategists must pay heed to the environment in which they will be planning and employing cyber operations.

⁴² JP 3-13, *Information Operations*, IV-9 – IV-10.

⁴³ Clarke, *Cyber War*, 143.

Summary

The organization of the forces, units, and agencies that have a role within cyberspace must foster prompt solutions to future problems and threats. These organizations must promote innovation that “fosters the values of cooperation and problem solving and encourages flexibility, diversity, and innovation.”⁴⁴ The military’s first step in promoting these elements is made possible through the organization of cyberspace resources; the second is the development of training military warriors to enable cyber power. The challenge these organizations will have in the future is finding the proper C2 relationships to effectively utilize cyber forces and provide cyber power to the warfighter.

CYBERCOM’s mandate is to conduct full-spectrum operations in cyberspace, “to defend American military networks and attack other countries’ systems.”⁴⁵ Is the unified command model appropriate within the context of cyberspace? Yes, and no. Military command establishes hierarchical command and control, but the nature of cyberspace requires the separation of attack and security. The following two chapters will discuss these two organizational pillars the military has constructed in cyberspace.

⁴⁴ R. A. Ratcliff, *Delusions of Intelligence—Enigma, Ultra, and the End of Secure Ciphers* (New York: Cambridge University Press, 2006), 236.

⁴⁵ Editorial, “War in the fifth domain”, *Economist* (1 July 2010), <http://www.economist.com/node/16478792> (accessed 15 May 2012).

Chapter 3

Cyber Defense—Decentralized Command & Control

Or

Fighting Through the Attack

The most fertile areas always attracted the strongest attack, and therefore required the strongest defence; and between the fertile and the infertile areas it was possible to draw the line which for strategical purposes was definite and constant. The fertile areas were the terminals of departure and destination where trade tend to be crowded, and in a secondary degree the focal points where, owing to the conformation of the land, trade tends to converge.

—Julian S. Corbett
Some Principles of Maritime Strategy

As the previous chapters have shown, the concept of cyberspace is incredibly complex and quite ambiguous. Its nature has only added to the fog that makes strategy difficult. Alone and within one's own system, these complexities can be significant, but cyberspace is not just an internal function and outside influence is a significant piece of this puzzle. It is common for the United States government's global information grid (GIG) to be attacked millions of times each day. Recently, a government security report stated that in one month, March of 2010, over 1.6 billion cyber attacks occurred against US government agencies, the majority of which originated outside of the country.¹ In fact, in April 2012 the Government Accountability Organization announced that cyber attacks against American federal agencies has

¹ Michael Evans and Giles Whittell, "Cyberwar declared as China hunts for the West's intelligence secrets," *Times* (London, 8 March 2010), as referenced in Chris C. Demchak and Peter Dombrowski, *Rise of a Cybered Westphalian Age*, Strategic Studies Quarterly (Spring 2011), 38.

increased 680% in the last six years.² These networks require significant levels of cyber security, and these defensive measures require decentralized control in order to command daily network security efforts. Cyberspace has now become what Julian Corbett explained as the most fertile areas.³ Cyberspace attracts a significant and specific threat, and the military must build the strongest defense to confront these attacks. Attacks from cyberspace “offer a means for potential adversaries to overcome overwhelming US advantages in conventional military power and to do so in ways that are instantaneous and exceedingly hard to trace.”⁴ This advantage held by the adversary makes it imperative that the US military have the capability to stand its cyber ground and protect its networks. Nowhere is a network more vulnerable and a commander’s capability to defend cyber more important than in the case of the joint force commander (JFC).

This chapter pulls extensively from joint doctrine, specifically Joint Publication 3-01, *Joint Doctrine for Countering Air and Missile Threats*, 19 October 1999, and Joint Publication 3-30, *Command and Control of Joint Operations*, 12 January 2010. These publications provide joint guidance for commanders to conduct successful joint operations.⁵ This chapter examines the command and control (C2) of cyber defense, and the role decentralized execution plays in a commander’s ability to secure his command networks and conduct successful joint operations to counter cyber threats allowing his command to continue day-to-day operations and conduct theater specific missions.

² Sydney J. Freedberg Jr., “Cyber Attacks on Feds Soar 680% in 6 Years: GAO,” America Online Defense (24 April 2012), <http://defense.aol.com/2012/04/24/cyber-attacks-on-feds-soar-680-in-6-years-gao/> (accessed 24 April 2010).

³ Julian S. Corbett, *Some Principles of Maritime Strategy* (Annapolis, MD: Naval Institute Press, 1988), 261.

⁴ William J. Lynn III, *Defending a New Domain: The Pentagon’s Cyberstrategy*, Foreign Affairs (September/October 2010), <http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain> (accessed 15 March 2012).

⁵ Department of Defense, Joint Publication 3-01, *Joint Doctrine for Countering Air and Missile Threats*, (19 October 1999), i.

The first section, *The Defense*, will introduce the concept before it is applied specifically into the cyber domain. In the second section, *Active Defense*, this chapter begins to build on the concept of defense in cyberspace, specifically as it applies to a commander's network. The final section of this chapter, *Decentralized Control of Cyber Defense*, examines what command responsibilities and relationships must exist in order for a commander to properly defend his networks. Now, in the cyber age, that same commander is required to conduct successful joint operations to counter cyber threats and cyber attacks. This chapter concludes by proposing specific command changes required by expanding cyber threats and a doctrinal change that will improve the military's capability to conduct cyber defense operations. Specifically, doctrine should allow unified, subordinate unified, or JFCs to establish an Area Cyber Defense Commander (ACDC).

The Defense

If the offensive were to invent some major new expedient—which is unlikely in view of simplicity and inherent necessity that marks everything today—the defensive will also have to change its methods.

—Carl von Clausewitz
On War

In *On War*, Carl von Clausewitz proclaimed that the defensive form of war was both easier and stronger than the offensive form of war.⁶ This divide between the offense and the defense would become a point of contention among classic military strategists such as Clausewitz, Julian Corbett, Antoine-Henri Jomini, and Alfred Thayer Mahan. Corbett agreed with Clausewitz that defense “being negative in its aim” was the stronger form of war, but concluded that, “The Offensive, being positive

⁶ Carl von Clausewitz, *On War* (Princeton, NJ: Princeton University Press, 1976), 357-359.

in its aim is naturally the more effective form of war.”⁷ Jomini explained that if attacked, one should use all means to defend. “The defensive army . . . should endeavor . . . to neutralize the first forward movement of its adversary, protracting operations as long as possible while not compromising the fate of the war, and deferring a decisive battle until the time when a portion of the enemy’s forces are either exhausted by labors, or scattered.”⁸ In warfare, however, defense is not the only answer nor does it stand independently.

Mahan argued that, while important, defense should not be independent of offense because defense only allowed a commander to maintain his position and did not allow a commander to gain additional positions. Mahan conceded that the defense was a stronger form of warfare because, “they interpose such passive resistance to the assailant as to enable smaller force to hold in check a larger.”⁹ Defensive actions, however, still required offensive actions. Mahan explained, “Napoleon said that no position can be permanently maintained if dependent upon defense only; if not prepares for offensive measures, or if it fails to use them. The enemy must be disturbed or he will succeed.”¹⁰ This union of offense and defense is captured with the idea of active defense, which will be defined in the following section. This concept of active defense is not possible without first having passive defense measures.

Passive defense allows one to absorb an attack. It is “all measures [other than active defense], taken to minimize the effectiveness of hostile air and missile threats against friendly forces and assets.”¹¹ In the case of cyberspace, these measures fall under the realm of network security.

⁷ Corbett, *Some Principles of Maritime Strategy*, 310.

⁸ Antoine-Henri, Baron de Jomini, *The Art of War* (Mineola, N.Y.: Dover Publications, 2007), 296.

⁹ Alfred Thayer Mahan, *Mahan On Naval Strategy: Selections from the Writings of Rear Admiral Alfred Thayer Mahan*, ed. John B. Hattendorf (Annapolis, Md.: Naval Inst Pr, 1991), 127.

¹⁰ Mahan, *Mahan On Naval Strategy*, 121.

¹¹ JP 3-01, *Joint Doctrine for Countering Air and Missile Threats*, I-3.

Actions that harden the defenses of commanders' networks are examples of passive defense. These inherent barriers protect from external manipulation, and include the basic maintenance and operations of the network. If attacked, the passive defense responds by closing and securing the vulnerability.

Passive defense in cyberspace is the responsibility of every commander. Passive defense "provides individual and collective protection for friendly forces and critical assets."¹² This statement holds true for cyber just as it does for air defense. Joint Publication 3-01, lays out specific passive measures one can take to improve one's defensive posture for countering air and missile threats. These passive measures can also be adapted to the specific nature of cyber:¹³

1. *Camouflage, concealment, and deception (CCD)*: These measures are used in an attempt to deny the enemy an accurate location of friendly targets in cyberspace. This can include the location of data and the location of entry points into a network. CCD is also used to present false information to the enemy, such as parallel faked networks or data used as bait. These honey pots are set up to trap an attacker by dictating his actions in your network. Honey pots can be used as early warning or surveillance tools, and monitor the tactics of the enemy. These passive measures can be conducted continuously or adapted in response to a specific threat warning.
2. *Hardening*: Valuable assets in cyberspace should be hardened to protect against attack. This is not physical hardening (which is beyond the bounds of cyberspace) but the hardening of software and network systems. These valuable assets include specific sections of networks and specific data that is deemed a

¹² JP 3-01, *Joint Doctrine for Countering Air and Missile Threats*, V-2.

¹³ These passive measures are each quoted from the joint pub but changed so that they reflect the nature of cyber defense as opposed to air defense. JP 3-01, *Joint Doctrine for Countering Air and Missile Threats*, V-2.

higher priority. These passive measures include techniques such as firewalls and any techniques that make it difficult for an adversary to gain entry into a friendly system.

3. *Reconstitution*: This is the capability for rapid repair of damage from an enemy attack that allows a commander to fight through such an attack. Once an incident or an attack occurs, the cyber network must be able to continue providing cyber power and returned to combat readiness. Examples of reconstitution include cyber teams closing network vulnerabilities, tracking foreign entities within the network, eliminating foreign entities, and fixing the damage caused by the cyber attack.
4. *Redundancy*: Duplication of critical network capabilities enables vital systems to continue operating when critical nodes are attacked, damaged, or destroyed. This can include multiple networks and multiple pathways between systems. Redundant systems are critical in a command.
5. *Detection and warning systems*: This provides maximum reaction time for friendly forces to take appropriate defensive measures. Detections and warnings must be communicated throughout a command and beyond to defend against new and adapting cyber threats.
6. *Dispersal*: This complicates an enemy's ability to target cyber systems. These measures include multiple servers in multiple locations with multiple lines of communication between them.

These passive measures must be in place to defend against the multiple attacks that networks should be expected to receive. These capabilities are the responsibilities of all commanders in the joint force, and should be inherent to their cyber systems and plans.

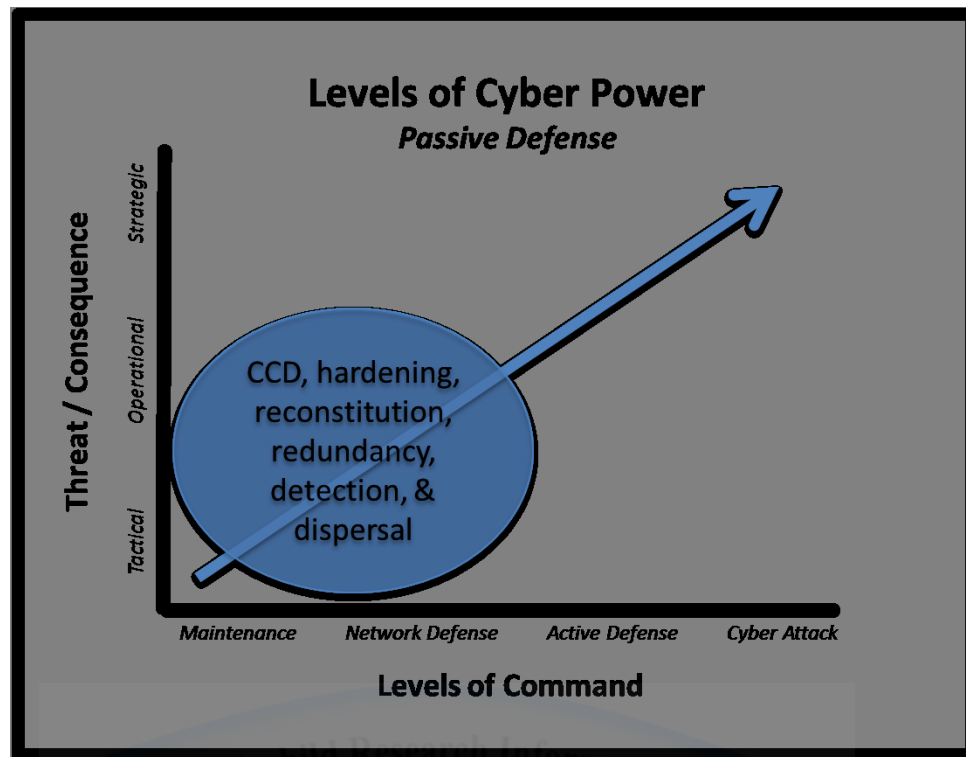


Figure 9: Cyber Power - Passive Defense

Source: Author's Original Work

The defense of network capabilities is first and foremost a strategic imperative. Unfortunately, cyber defense seems to be widely ignored. Air and space capabilities are overly reliant on cyber support. The synchronization of military capabilities requires substantial networks, and these capabilities can be blunted by cyber attacks. The American military often relies on the offense, and finds it difficult to break this paradigm and admit that defense is strategically imperative. Defense in cyber *is* imperative. Corbett explained that the defensive form of war increased the vulnerabilities of the attacker. “Seeing that the defensive is a stronger form of war than the offensive, it is *prima facie* [first face] better strategy to make the enemy come to you than to go to him and seek a decision on his own ground.”¹⁴ As the following sections will show, defense is the strongest form of cyber warfare, but only if it is

¹⁴ Corbett, *Some Principles of Maritime Strategy*, xxi.

allowed to be paired with the offensive, in the form of active defense, and if it is allowed to be controlled at the ground level, by the ACDC.

Active Defense

If defense is the stronger form of war, yet has a negative object, it follows that it should be used only so long as weakness compels, and be abandoned as soon as we are strong enough to pursue a positive object.

—Carl von Clausewitz
On War

The offensive and defensive forms of war are tightly bound. Commanders require the ability to “pass instantaneously from the defensive to the offensive without any warning.”¹⁵ In order to protect military networks, passive defense must be linked with active defense. Active defense confronts would be attackers or those currently attacking. Joint Publication 3-01 defines active defense as “direct defensive action taken to destroy, nullify, or reduce the effectiveness of hostile . . . threats against friendly forces.”¹⁶ By establishing networks inherent to mission success, the military has, in a sense, left the initiative up to its adversary. The active defense allows the defender to gain some initiative as well. Clausewitz explained that, “. . . every engagement, large or small, is defensive if we leave the initiative to our opponent and await his appearance before our lines.”¹⁷ In cyber, unfortunately, sometimes that is exactly what one is forced to do; but, by employing an active defense, one “can employ all offensive means without losing the advantages of the defensive—that is to say the advantages of waiting and the advantages of position.”¹⁸

¹⁵ Corbett, *Some Principles of Maritime Strategy*, 330.

¹⁶ JP 3-01, *Joint Doctrine for Countering Air and Missile Threats*, I-3.

¹⁷ Clausewitz, *On War*, 358.

¹⁸ Clausewitz, *On War*, 358.

Active defense is akin to hunting, or the pursuit of an attacker. “A pursuit should generally be as boldly and actively executed as possible.”¹⁹ This requires the sensing of the environment and the enemy’s presence or actions. This hunting should disrupt, degrade, disable, destroy, or usurp control of the enemy’s capability to attack the network one is trying to defend. Active defense means traveling outside of the lines one is attempting to defend. A defensive team may be required to go outside of a network to stop an attack from happening. Corbett explained that the true purpose of the defense was to provide a chance to strike the enemy. “The strength and the essence of the defensive is the counter-stroke. A well designed defensive will always threaten or conceal an attack.”²⁰

Active defense missions in cyberspace are not the responsibility of every joint commander. Each commander does not hold the forces or capabilities necessary to “protect selected assets and forces from attack by destroying enemy” forces during the attack.²¹ Active defense operations should be subject to the cyber defense procedures laid out by the ACDC. These procedures can include the following:²²

1. *Area defense*: This technique uses a combination of cyber active defense systems to defend broad areas, such as an expeditionary network. These techniques include utilizing passive defense measures to detect and warn of an attack, and identify details of the attack that are necessary in order to counter the threat.
2. *Point defense*: This technique protects limited areas, normally in the defense of vital cyber elements. Point defense may be

¹⁹ Jomini, *The Art of War*, 221.

²⁰ Corbett, *Some Principles of Maritime Strategy*, 310-311.

²¹ JP 3-01, *Joint Doctrine for Countering Air and Missile Threats*, V-3

²² These active measures are each quoted from the joint pub, but changed so that they reflect the nature of cyber defense as opposed to air defense. JP 3-01, *Joint Doctrine for Countering Air and Missile Threats*, V-3 – V-4.

taken in response to a breach in the system, and set up to protect that vulnerability and track down the attacking entity. This type of active defense can also protect a known weakness that has been identified within the network.

3. *Self defense*: These operations are those beyond the self-defense measures of passive defense. Active self defense allows cyber forces to protect their networks against direct attack or threats of attack using organic cyber systems. At times self defense may require active defensive measures *outside of one's network*. These actions will come from the authority of the ACDC or delegated downward through specific rules of engagement (ROEs).

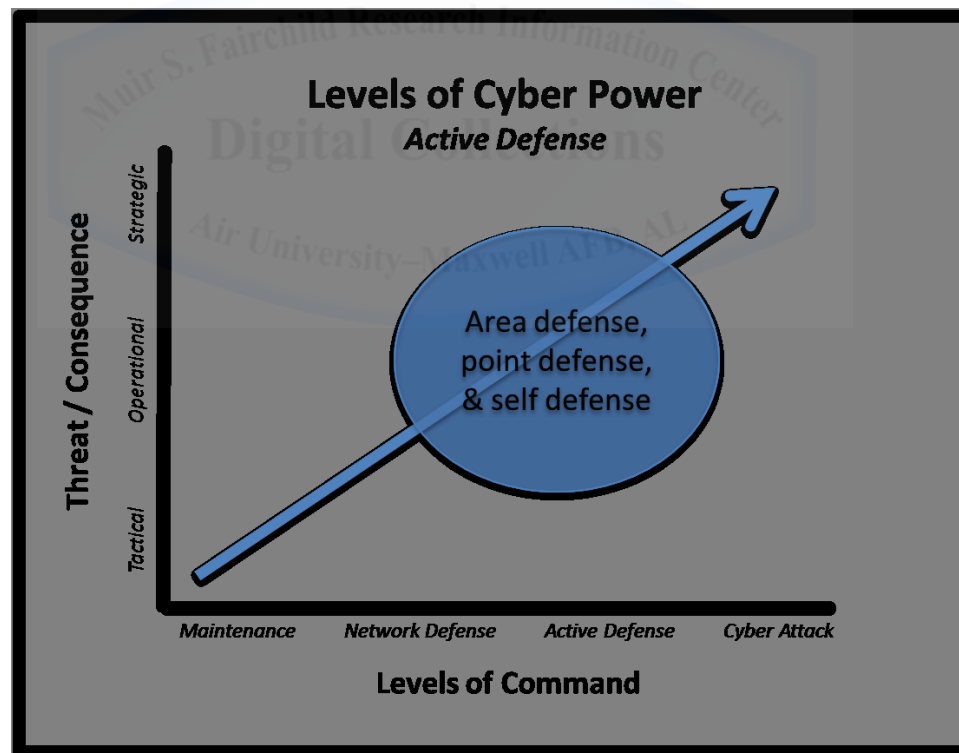


Figure 10: Cyber Power - Active Defense

Source: Author's Original Work

These active defense measures are not specifically internal to the commander's networks. At times it will be necessary for active defense forces to go beyond their own network either to target an attacker or gain intelligence of an attacker in order to harden future defenses. However, actions outside of the commander's networks come precariously close to cyber attack and those authorities currently held by Cyber Command (CYBERCOM). In these cases, the ACDC must be in communication with both his JFC and CYBERCOM in order to interpret the level of attack and the level of cyber force necessary to thwart that attack. Many of the details required for these relationships should be included in cyber ROEs.

The right to self defense is normally inherent in the ROE, but in cyberspace this has been a confusing point. "You have the right to self-defense, but you don't know how far you can carry it and under what circumstances, and in what places," says General James E. Cartwright Jr., retired vice chairman of the Joint Chiefs.²³ It is for this very case that the ACDC must set in place clear rules for cyber engagement, and be in command of the forces that would act in such a situation. This guidance must explain what cyber forces should do in the case of specific attack situations, whether that is run, fight, or hunt. Cyberspace remains ambiguous to the commander, and an ACDC would help clarify doctrinal command relationships and operational procedures.

Active defense not only protects one's networks, but can also influence enemies to act in such a way that will leave them vulnerable in the future. To assume the defensive "may mean that we see our way by using the defensive to force certain movements of the enemy which will enable us to hit harder," and "force the enemy to attack us in a position where he will expose himself to a counter-stroke."²⁴ Commander's

²³ Ellen Nakashima, "Cyber-intruder Sparks Massive Federal Response—and Debate over Dealing with Threats", The Washington Post (December 8, 2011) http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html (accessed 14 December 2011).

²⁴ Corbett, *Some Principles of Maritime Strategy*, 329-330.

networks are fertile areas. These networks are strategic centers of gravity, and should be protected like fortresses. The defenses of these strategic points “are absolutely necessary to the control of any theater of war.”²⁵

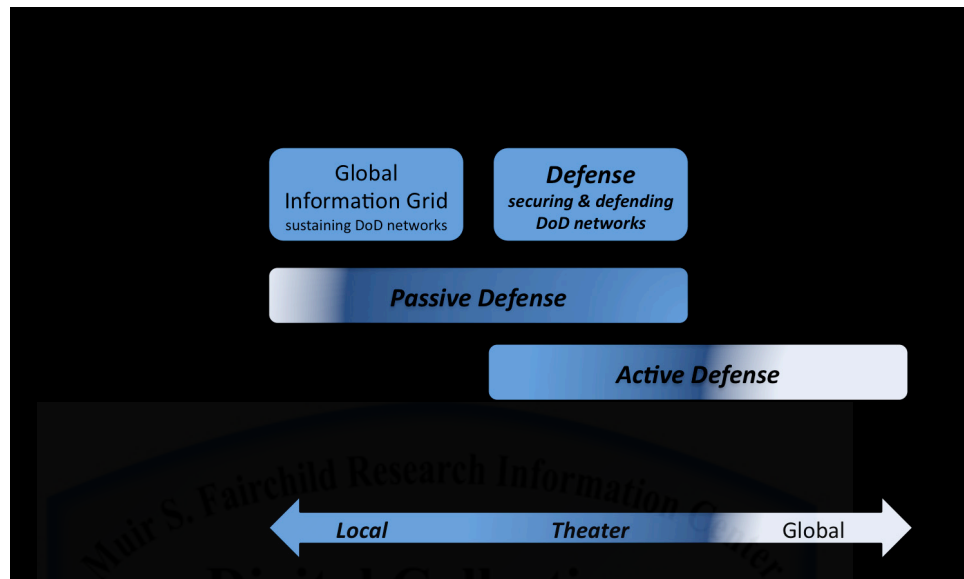


Figure 11: Cyber Defense Lines of Operation

Source: Author's Original Work

The intent of the ACDC is to provide both passive and active defensive measures to the JFC. This change in doctrine will provide command and control of defensive capabilities of an expeditionary network. It will warn a commander of an imminent or occurring attack, and provide the defensive measures necessary to thwart such an attack. Currently combatant commands have Network Control Centers (NCC), but do not have an active defense capability to include sensors or forces. In effect, expeditionary networks are the most vulnerable to attack, and the Department of Defense (DOD) does not have a plan to defend them. The ACDC would solve this problem by establishing relationships between the combatant commander and network defenders at

²⁵ Mahan, *Mahan On Naval Strategy*, 127.

CYBERCOM.

The ACDC is necessary to integrate theater cyber capabilities into theater combat plans. With cyber forces made available, the ACDC can establish and maintain a cyber environment that can support the other combatant commands. The ACDC can also coordinate long-range cyber fires in support of the JFC's concept of operations by coordinating with CYBERCOM for offensive measures support. Figure 3, *Area Cyber Defense Commander Responsibilities*, elaborates on the detailed relationship between the ACDC and the JFC and the ACDC's responsibilities.²⁶

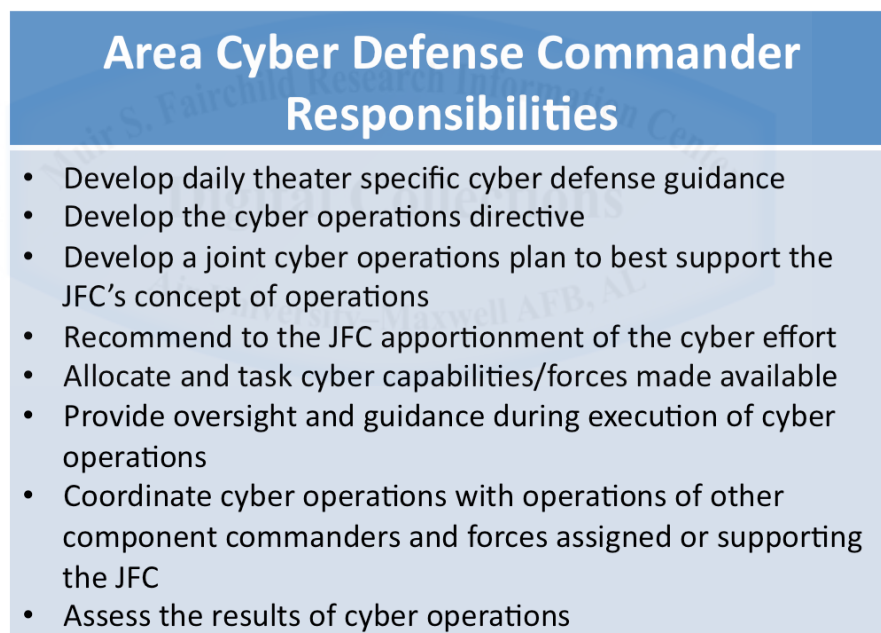


Figure 12: ACDC Responsibilities

Source: Author's Original Work

²⁶ These responsibilities mirror those of the JFACC as detailed in JP 3-30. "JFACC Responsibilities", Department of Defense, Joint Publication 3-30, *Command and Control of Joint Operations*, (12 January 2010), II-3.

Decentralized Control of Cyber Defenses

. . . decentralized execution of airpower [is] critical to its effective employment. Because of airpower's unique potential to directly affect the strategic and operational levels of war, it should be controlled by a single Airman who maintains the broad, strategic perspective necessary to balance and prioritize the use of a powerful, highly desired yet limited force.

—JP 3-30, *Command and Control of Joint Operations*

Just as airpower requires control of a single Airman, cyberspace requires the control of a single cyber-minded individual. A commander must have the authority and capability to secure and defend his own networks. This is not unlike a commander's authority to protect his area of responsibility (AOR) through air defense measures. With the growing complexity of computer networks, cyber capabilities, and adversary capabilities, cyber defense requires flexible and adaptable response options. A combatant commander must be provided the opportunity to designate an ACDC to defend the expeditionary network.

The Area Air Defense Commander (AADC) provides commanders with decentralized control of air defense. The AADC is "responsible for defensive counterair (DCA) operations, which include integrated air and missile defenses for the JOA [joint operations area]."²⁷ This responsibility can be assigned within a unified command, subordinate unified command, or joint task force. The AADC also develops air defense priorities and implements the area air defense plan. These responsibilities are accomplished by integrating the capabilities of multiple components, and, "because of their time sensitive nature, DCA operations require streamlined coordination and decision-making processes facilitated by the AADP [area air defense plan]."²⁸ The ACDC, in turn, should establish an integrated cyber defense system with a

²⁷ JP 3-30, *Command and Control of Joint Operations*, II-7.

²⁸ JP 3-30, *Command and Control of Joint Operations*, II-8.

concept of operations that includes cyber defense priorities, a cyber defense plan.

Normally, the AADC is the “component commander with the preponderance of air defense capability and the command, control, communications, computers, and intelligence capability to plan, coordinate, and execute integrated air defense operations.”²⁹ This may hold true as well for the ACDC, but in order to simplify the hierarchy, and ensure cyber capabilities are implemented properly, the ACDC should come from STRATCOM, specifically CYBERCOM.

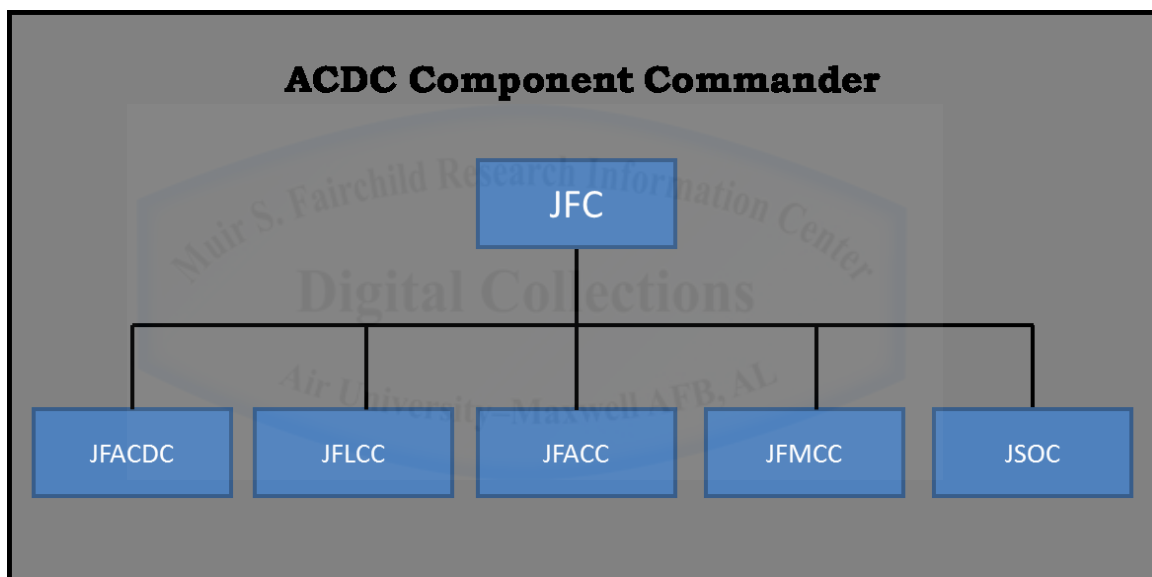


Figure 13: Joint ACDC Component Commander under the JFC

Source: Author's Original Work

Apportioned Capabilities

The JFC should apportion cyber capabilities to the ACDC for cyber defense missions, and determine the appropriate command authority over these capabilities. In the case of the AADC, air and naval forces provide tactical control (TACON) for offensive and defensive counter-air sorties. In the case of the ACDC, JFCs or CYBERCOM can provide cyber

²⁹ JP 3-01, *Joint Doctrine for Countering Air and Missile Threats*, vii.

forces. In addition, the ACDC would normally be the supported commander for defensive cyber operations. With this responsibility, the ACDC would plan, organize, and execute defensive cyber operations across the AOR. To facilitate synchronization, as he does for the command and control of air defense, “the JFC establishes priorities that will be executed throughout the theater,” including cyber commander’s area of operations.³⁰ The ACDC would act in coordination with the other component commanders, and have the latitude to plan and execute the JFC-prioritized cyber defense operations.³¹

Defensive cyber forces assigned to an ACDC will remain under the combatant command (COCOM) of their respective geographic or functional commands. The ACDC will then exercise operational control (OPCON) of all assigned cyber forces. The ACDC may also establish defensive cyber task forces to manage cyber requirements, and employ TACON of cyber forces. Also, CYBERCOM can provide cyber forces on a temporary basis to other commanders for operational employment. When these cyber forces are transferred they are attached to “the gaining combatant command with the GCC normally exercising OPCON over them.”³²

³⁰ JP 3-01, *Joint Doctrine for Countering Air and Missile Threats*, II-1

³¹ JP 3-01, *Joint Doctrine for Countering Air and Missile Threats*, II-1

³² Department of Defense, Joint Publication 3-05, *Special Operations* (18 April 2011), III-2.

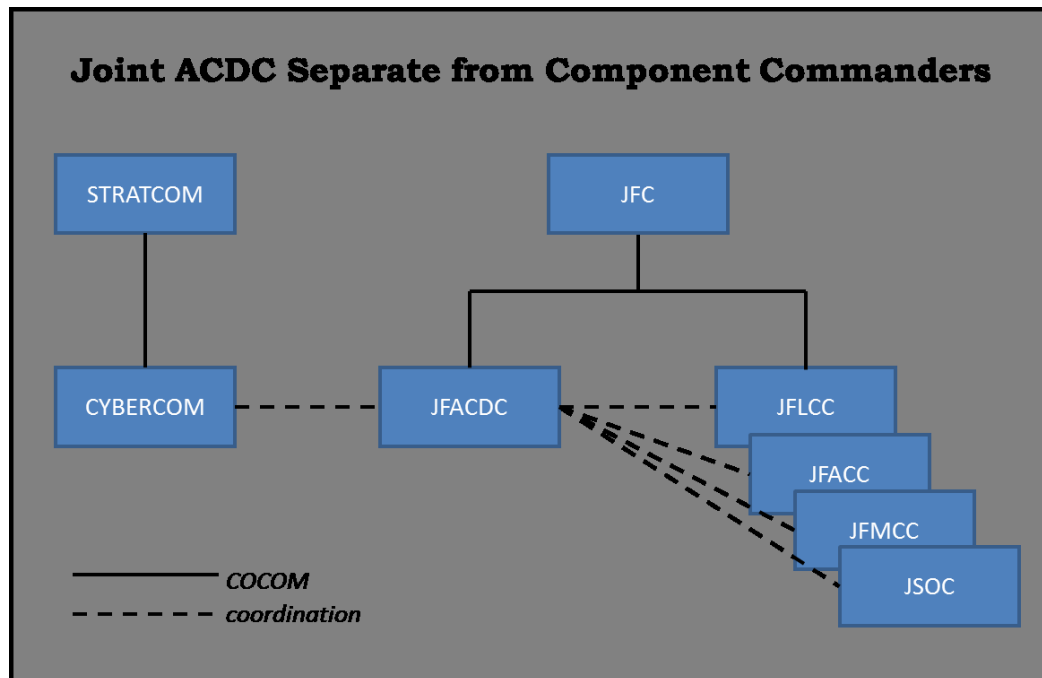


Figure 14: Joint ACDC - Non-Component Commander

Source: Author's Original Work

The Joint Force Commander

According to Joint Publication 3-01, the “JFC exercises combatant command (command authority) or operational control (OPCON) over assigned or attached forces to ensure unity of effort to counterair and missile threats.”³³ In the same light, the JFC must utilize the ACDC to ensure the unity of effort for assigned cyber defense forces. The JFC “provides authoritative direction to subordinate commanders on objectives, priorities, missions, and apportionment of joint capabilities and forces.”³⁴ The JFC’s primary responsibilities as they relate to cyber should be:

1. Develop and maintain a system to unify the employment of subordinate cyber forces in carrying out assigned defensive cyber missions.

³³ JP 3-01, *Joint Doctrine for Countering Air and Missile Threats*, II-2.

³⁴ JP 3-01, *Joint Doctrine for Countering Air and Missile Threats*, II-2.

2. Develop and produce joint operation plans for cyber passive and active defense missions.
3. Assign tasks, functions, and responsibilities to, and direct coordination among, the subordinate commands to ensure unity of effort in accomplishing counter cyber missions.
4. Establish, coordinate, and disseminate cyber ROE to all subordinate commanders.
5. Define the support relationship between the ACDC and supporting or supported commanders.³⁵

The JFC designates a Joint Forces Air Component Commander (JFACC) to integrate air capabilities of joint air assets. This normally involves assigning the responsibilities of the JFACC, AADC, and the Airspace Control Authority (ACA) to a single individual. As this relates to the cyber domain, the ACDC will certainly have operations and cyberspace control that require synchronization, and this will most certainly require subordinate commanders and authorities. The ACDC's *primary* responsibilities should be:

1. Develop, coordinate, and integrate the joint counter cyber plan with operations of other components for JFC approval.
2. Make a cyber apportionment recommendation to the JFC, after consulting with other component commanders.
3. Provide centralized direction for allocating and tasking defensive cyber capabilities and forces made available by the JFC.
4. Provide strategies to neutralize enemy cyber threats while preserving friendly defensive cyber capabilities.
5. Provide timely warning of cyber attacks.³⁶

³⁵ These responsibilities are quoted from the primary responsibilities of the JFC as they apply to the counter-air mission. Those that did not apply to cyber were omitted and, the remaining responsibilities were changed to reflect the nature of war in cyber. JP 3-01, *Joint Doctrine for Countering Air and Missile Threats*, II-2, II-6.

Effects in a military campaign require an understanding and intimacy of the battlefield. The chain of command must be fast enough to react to attacks. It must be adaptable to changing threats. This requires commanders to have the ability to rapidly reprogramming for vulnerabilities to new technologies. New technologies are common in the cyber environment where a large commercial market maintains a fast product cycle. Many of these vulnerabilities may be specific to his AOR.

Defense of a command's network depends on local control. In order for this to occur, CYBERCOM must release command of its defensive authorities, and allow the ACDC OPCON to execute separate plans and operations specific to a command's AOR and network. A commanders networks, and therefor his command, is reliant on the local control of this defense. As Corbett explained, "the defence could only fall when our means of local control was destroyed."³⁷ A commander must control his own network in order to ensure its defense.

³⁶ These responsibilities are quoted from the primary responsibilities of the JFACC as they apply to the counter-air mission. Those that did not apply to cyber were omitted and the remaining responsibilities were changed to reflect the nature of war in cyber. JP 3-01, *Joint Doctrine for Countering Air and Missile Threats*, II-4 - II-5.

³⁷ Corbett, *Some Principles of Maritime Strategy*, 265.

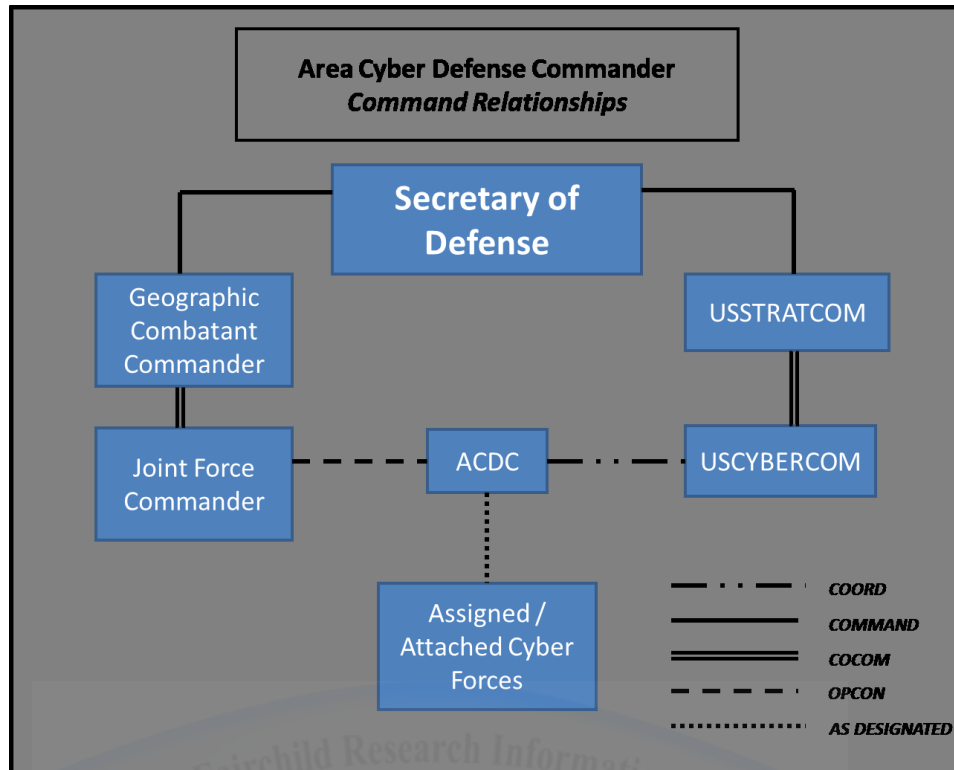


Figure 15: ACDC Command Relationships

Source: Author's Original Work

Summary

The act of attack, particularly in strategy, is thus a constant alternation and combination of attack and defense. The latter, however, should not be regarded as a useful preliminary to the attack or an intensification of it, and so an active principle; rather it is simply a necessary evil, an impending burden created by the sheer weight of the mass. It is its original sin, its mortal disease.

—Carl von Clausewitz
On War

As cyber threats continue to adapt and evolve to the security environment, military forces are required to build more flexible and integrated responses to counter them. Cyber defense is imperative to the success of practically any military mission. The purpose of the cyber

defense mission is to maintain a degree of cyber control that allows freedom of action in cyber and the security of the command's networks. The goal of cyber defense is to enhance the commander's ability to employ actions in cyberspace. Proper defense of expeditionary networks "maximize the effectiveness of combat operations without adding undue restrictions and with minimal adverse impact on the capabilities of any Service of functional component."³⁸ But proper defense is not yet inherent to JFCs.

This chapter proposes the establishment of the Area Cyber Defense Commander. This new position will hold the authority and responsibility of defensive cyber actions and cyber forces within a specified AOR. The overarching objective of the ACDC is the defense of an AOR's networks. While not service specific, this command should hold the preponderance of cyber forces and have the ability to command them. The ACDC will establish an overall defense plan that includes both active and passive defensive measures. These measures will allow JFC's to integrate cyber effects into the land, sea, and air domains. At times, active measures—those that require cyber forces to extend beyond their own network—require additional responsibilities or authorities beyond the ACDC. Active measures beyond one's network begin to blur into the realm of cyber attack—an authority that the ACDC does not hold. These offensive actions and their implications will be examined and explained in the following chapter.

³⁸ JP 3-01, *Joint Doctrine for Countering Air and Missile Threats*, III-1.

Chapter 4
Cyber Offense—Centralized Command & Control
Or
Long-Range Strategic Cyber Fires

The offensive is nearly always advantageous: it carries the war upon foreign soil, saves the assailant's country from devastation, increases his resources and diminishes those of his enemy, elevates the morale of his army, and generally depresses the adversary.

—Antoine-Henri, Baron de Jomini
The Art of War

The question of appropriate command of attacks in cyberspace poses multiple challenges to military leadership. Count Helmuth von Moltke, Prussian general and war strategist, explained that a commander must be allowed “complete freedom to act according to his own judgment.”¹ He believed that conducting war from the planning table and issuing orders from a distance to be a grave mistake. In cyberspace, this idea holds true for passive and active defensive measures, but this is in a context of warfare where estimates of current local conditions have an integral part of the commander's decision-making process. In today's globalized environment—one riddled with cyberspace complexities that can both shrink and expand these local conditions—the process of offensive attack has become a difficult task and can easily leap from local to global implications. These global implications emphasize the importance and requirement of long-range cyber fires. It is often said that a strong offense makes for a good defense. So, in order to disrupt one's enemy and protect one's own networks, militaries must have offensive cyber based capabilities to attack enemy networks.

¹ Daniel J. Hughes (editor), *Moltke—On the Art of War, Selected Writings* (New York: Ballantine Books, 1993), 77.

The United States military relies on cyberspace for key functions in everyday operations. If these functions were interrupted the military would have significant problems accomplishing not only day-to-day activities, but also, its mission of defending the security of its nation. Therefore, “it is critical that cyber infrastructures and resources be incorporated into the command and control hierarchy.”² Adding to this complexity is the fact that the military is not in charge of the integral parts of cyberspace that would allow them access to actively defend and attack this domain. This is not necessarily a negative situation, just different from the way militaries are accustomed to operating. The military wants unfettered access, but they often rely on commercial technologies that are shared with the public and therefore vulnerable to its enemies.³ Cyberspace consists of multiple sections and networks: government, military, corporate, and civilian. Effective defense relies heavily on the control of one’s own network and effective offense requires traveling beyond the bounds of one’s castle walls. There is certainly a fine line between defensive and offensive military actions in cyberspace.

This chapter examines the command and control (C2) of cyber offense, and the role that a centralized structure plays in a commander’s ability to conduct successful offensive joint operations in cyberspace. Regardless of command structure and in the current strategic environment, cyberspace requires the centralized control of cyber attack. The implications of actions in cyberspace can have devastating strategic effects, and can be interpreted much differently than what was actually intended. Cyber’s strategic implications are so high that new organizations are necessary for its C2. The first section of this chapter, *The Attack*, introduces the concept of this form of war. In the second

² Robert F. Erbacher, *Extending Command and Control Infrastructure to Cyber Warfare Assets*, http://www.researchgate.net/publication/4210741_Extending_command_and_control_infrastructures_to_cyber_warfare_assets (accessed 20 January 2012).

³ Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins Publisher, 2010), 93.

section, *Offense in Cyber*, the concept of attack in cyberspace builds upon this frame, describes what cyberspace provides a commander, and how that applies to specific areas of responsibilities (AORs). Finally, the *Centralized Control* section examines what command responsibilities and relationships must exist in order for a commander to effectively attack in cyberspace. This examination will include two centrally controlled command structures: the Joint Space Operations Center (JSPOC) and the Special Operations Global Mission Support Center. This chapter concludes by proposing specific command changes required by ever expanding cyber capabilities, and a doctrinal change that will improve the military's capability to conduct offensive cyber operations. Specifically, doctrine should allow strategic military offensive cyber operations to be controlled by a single commander, the Cyber Command (CYBERCOM) commander, at a global and centralized location, a Strategic Attack Cyber Center (SACC).

The Attack

Command enables the army to carry out its proper mission, which is to inflict the maximum amount of death and destruction on the enemy within the shortest possible period of time and at minimum loss to itself.

—Martin van Creveld
Command in War

In order for one to begin to understand attack in cyberspace, one must shift their viewpoint from the defense. In a defensive action, measures and movements are “more likely to fan out from the center towards the periphery,” and in an offensive action the attacker converges towards the center.⁴ The attack is the opposite of the defense, and in

⁴ Carl von Clausewitz, *On War* (Princeton, NJ: Princeton University Press, 1976), 391.

war, the action of the attacker meets the reaction of the defender. The two forms of war are oppose each other, and the “two ideas form a true logical antithesis, each complimentary to the other, then fundamentally each is implied in the other.”⁵ While the defense may protect a commander’s local network, it does not ensure victory outside of that AOR. Victory in war must be “sought by offensive measures, and by them only can be insured.”⁶ These offensive measures dominate actions in cyberspace outside of one’s own networks. It is only then, through the “power of the offensive action” that the offense “is the dominant factor in war.”⁷ The offense and defensive forms of war are in parallel with one another, each insuring the other. The nature of cyber and its strategic environment require daily defensive operations—ones that should be inherent to a commander. But when an army attacks—outside its network and against an enemy’s organized forces—it is offensive cyber attack that will lead the way.

Offensive Targets

When considering the attack, the strategic problem is always where and when to apply the pressure. The intent of the attack is to weaken the adversary or deprive them of specific resources—commonly those resources that fuel the adversary’s power. Where one should attack an enemy is a common theme among military theorists and strategists, and targeting is often the objective of massive military undertakings. Carl von Clausewitz explained this concept by what he called centers of gravity (COGs). He explained these to be the dominating characteristic of either side, and “out of these characteristics a certain

⁵ Clausewitz, *On War*, 523.

⁶ Alfred Thayer Mahan, *Retrospect and Prospect. Studies in International Relations, Naval and Political* (1902), 152. Quoted in Alfred Thayer Mahan, *Mahan On Naval Strategy: Selections from the Writings of Rear Admiral Alfred Thayer Mahan*, ed. John B. Hattendorf (Annapolis, Md.: Naval Institute Press, 1991), xx.

⁷ Mahan, *Lessons of the War with Spain*, 82. Quoted in Mahan, *Mahan On Naval Strategy*, xxi.

center of gravity develops, the hub of all power and movement, on which everything depends.”⁸ COGs are what hold a force in balance, and therefore one’s offensive actions should be directed to create an imbalance in an enemy’s COG. Clausewitz emphasized that COGs are “the point against which all our energies should be directed.”⁹ Antoine-Henri Jomini described what this would look like on land: “The offensive army should particularly endeavor to cut up the opposing army by skillfully selecting objective points of maneuver; it will then assume, as the objects of its subsequent undertakings, geographical points of more or less importance, depending upon its first successes.”¹⁰ In cyberspace, however, offensive operations run the risk of becoming more ambiguous than just attacking the misconstrued and often simplified concept of centers of gravity.

Offense in Cyber

At first glance, command and control of cyber can seem overly complex and exceedingly ambiguous. Effects in a military campaign require an understanding and intimacy of the battlefield, but many military leaders and planners misunderstand what cyberspace is and what actions occur in that domain. Commanders must have cyber forces that are fast enough to defensively react to attacks, and adaptable enough to attack threats that change with technological advances. This involves rapid reprogramming when new vulnerabilities are identified or new technologies necessitate new defensive or offensive actions. The cyber lines of operation for the offense are detailed in the figure below.

⁸ Clausewitz, *On War*, 596.

⁹ Clausewitz, *On War*, 596.

¹⁰ Jomini, *The Art of War*, 296.

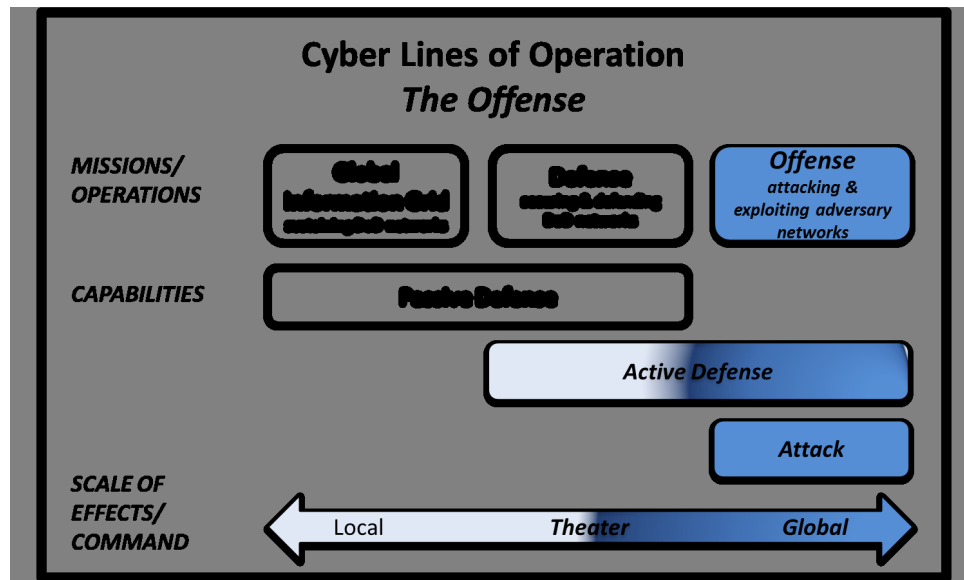


Figure 16: Offensive Lines of Operation

Source: Author's Original Work

Cyberspace has provided yet another degree of speed to the military commander. Electronic communications in the form of the telegraph and then the radio provided the commander with an incredible jump in capacity and capability. Before the electric telegraph, “the speed of communication over large distances was broadly limited to that of the fastest existing means of transportation.”¹¹ Historically, that meant by horse, maybe a carrier pigeon, or the slowest possibility, the human being. Electronic communication not only accelerated the ability of the commander to send out orders, it also allowed the commander to receive feedback and information at new speeds. This allowed the commander’s decisions to be based on up-to-date information rather than information that may have already been overcome by events. Cyberspace has provided another level of speed to the commander. This capability has accelerated information and command in such a significant way that technology has now become married to warfare. Alfred Thayer Mahan explained the importance of this concept when he proclaimed, “The true

¹¹ Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), 94.

speed of war is not headlong precipitancy, but the unremitting energy that wastes no time.”¹² But this concept of speed in cyberspace only covers coordination or the reporting of intelligence, not direct long-range offensive attack.

Attack in cyberspace holds many of the same characteristics that cyberspace provides the commander, most notably speed. And while the speed of the attack is often the advantage, there are often more complexities beneath the surface of these long-range fires. Attacks in cyber can have some significant disadvantages. While the speed of implementation is high, the speed of planning an attack is not. The ease of access into the cyber domain has created an environment where anonymity rules and the lack of jurisdiction has encouraged attacks to become commonplace. Understanding a target in cyberspace requires footprinting, or in-depth study and intelligence gathering of computer systems and networks. The fundamental challenges in cyber attack “consist of access, stealth and effects.”¹³ Access involves delivering the effect into an adversary’s network not to mention avoiding getting caught and understanding the second and third order effects an attack may hold. On a final note, cyber offense can also be considered a one-trick pony. Long range cyber fires employ “network-based capabilities to destroy, disrupt, corrupt, or usurp information resident in or transitioning through networks.”¹⁴ However, once it has been decided to use a specific technique of attack, that avenue is now public domain and it can be assumed that network defenders will ensure their networks are no longer vulnerable to those specific types of attacks. Which begs the question: Is the offense the overriding force in cyberspace?

¹² Mahan, *Lessons of the War with Spain*, 83. Quoted in Alfred Thayer Mahan, *Mahan On Naval Strategy*, xxix.

¹³ Kamal T. Jabbour, Dr., ST, *50 Cyber Questions Every Airman Can Answer* (Air Force Research Laboratory, 7 May 2008), 12.

¹⁴ Jabbour, *50 Cyber Questions Every Airman Can Answer*, 9.

Is Offense Dominant in Cyberspace?

As opposed to the defensive that is centered on reaction, the offensive form of war focuses on gaining an advantage by attempting to take the initiative. Clausewitz explained that “Just as the commander’s aim in a defensive battle is to postpone the decision as long as possible in order to gain time, the aim of the commander in an offensive battle is to expedite the decision.”¹⁵ Defensive actions are easier in war and also easier in cyberspace. And while these defensive actions are vital because they allow for offensive action, they are nonetheless still the weaker form of war. Clausewitz continues, “The defensive form of warfare is intrinsically strongest than the offensive,” because this form “has a negative object.”¹⁶ This distinction between the offense and the defense remains a common thread among strategists. Naval strategist Julian Corbett proclaimed that, “The Defensive, being negative in its aim, is naturally the stronger form of war,” and “the Offensive, being positive in its aim is naturally the more effective form of war.”¹⁷ This distinction holds true in cyberspace. Defense in cyberspace is the strongest form of cyber warfare because the military relies so heavily on its networks, and is therefore required to secure them. Offense in cyberspace, on the other hand, is the more effective form of war because it attacks the enemy and weakens its resources.

John Sheldon, cyber strategist and professor at the Air Force’s School of Advanced Air and Space Studies (SAASS), argues yes, the offense is the dominant form of war in cyberspace. He defends his argument by explaining that the application of defense is being applied incorrectly in cyberspace, the nature of cyberspace allows for inherent advantages to the attacker, and societal dependence on the domain provides an incredible target set. Current defense postures in

¹⁵ Clausewitz, *On War*, 531.

¹⁶ Clausewitz, *On War*, 358.

¹⁷ Julian S. Corbett, *Some Principles of Maritime Strategy* (Annapolis, MD: Naval Institute Press, 1988), 310.

cyberspace lean towards threat detection and not actual defense. Sheldon explains that the application of defense is being applied incorrectly in cyberspace: “network defenses rely on vulnerable protocols and open architectures, and the prevailing network defense philosophy emphasizes threat detection, not fixing vulnerabilities.”¹⁸ So, while strategists argue that the defense is the strongest form of war, cyber forces are not yet taking advantage of its inherent strength.

Next, Sheldon uses the nature of cyberspace to show that the offense holds an inherent position of advantage over the defense. In the argument between the offense and the defense, speed, range, and signature all benefit the attacker. The defender, on the other hand, must accept a great number of vulnerabilities when reliant on cyberspace. It is the speed of action in cyberspace makes all the difference: “attacks in cyberspace occur at great speed—for all intents and purposes to a human observer they seem instantaneous—putting defenses under immense pressure, as an attacker has to be successful only once, whereas the defender has to be successful all the time.”¹⁹ After speed, range in cyberspace makes it easier to attack and more difficult to defend. Different from other domains, in cyberspace, “range is not an issue,” and “attacks can emerge literally from anywhere in the world.”²⁰ The third characteristic of cyber attack, signature, creates problems for the defender. In cyberspace an attacker can remain relatively anonymous, “thus complicating any possible response.”²¹ Therefor the cyber attacker holds three great advantages over the defender: speed, range, and signature.

Finally, the networking of civilian and military systems provides both powerful advantages and potential vulnerabilities because “the

¹⁸ John B. Sheldon, “Deciphering Cyberpower: Strategic Purpose in Peace and War” in *Strategic Studies Quarterly* (Summer 2011), 98.

¹⁹ Sheldon, “Deciphering Cyberpower,” 98.

²⁰ Sheldon, “Deciphering Cyberpower,” 98.

²¹ Sheldon, “Deciphering Cyberpower,” 98.

cyberdomain is unique in that it is human-made, recent, and subject to even more rapid technological changes than other domains.”²² Conflict in this new domain is different from action in or on the air, land, and sea. Where global powers have the preponderance of force in traditional military matters, in cyber, barriers of entry are more -open, access is more inexpensive, and maneuver is more anonymous. Sheldon explains that cyberspace is extremely difficult to defend because the world and its militaries are so dependent on what cyberspace provides. The military must defend these targets, “again placing great strain on the ability to successfully defend the domain.”²³ So while cyberspace provides militaries with advantages, it also provides its adversaries with additional targets.

Network Attack and Exploitation

Attack in cyberspace is divided between two avenues, one that causes actual changes in an adversary’s network and one that does not. Attack can disrupt, degrade, disable, or destroy a targeted network; while exploitation only collects information. The problem is that, in cyberspace, the line between this delineation is very fine. Exploitation can lead to incidental changes in networks or the perception that a network is being attacked. If exploitation is used to prepare the battlespace, then adversaries may take these types of actions as attacks and defend against them as they see fit escalating or accelerating a conflict beyond what was originally intended.

Offensive cyber actions are slow to plan, and fast to execute. The use of cyber as an offensive weapon is difficult, just as any other weapon. It is hard to attack at a specific time. “If a cyber-attack is used as a

²² Joseph S. Nye, Jr., *The Future of Power* (New York: PublicAffairs, 2011), 124.

²³ Sheldon, “Deciphering Cyberpower,” 98.

military weapon, you want a predictable time and effect.”²⁴

There are two different types of targets available in cyberspace: geographic and non-geographic. With geographic related targets the adversaries are using specific cyber capabilities. These types of targets require tactical situational awareness, and must be integrated with the commander in the theater to synchronize the offensive effort. Non-geographic targeting involves targeting a system over a wide range, such as denial of service or complete system overload. Geographic targets can be attacked through active defense measures as described in the previous chapter, or can be attacked as part of the initial phase of a mission or operation. Non-geographic targets have a higher level of implications and require a specific command structure that is able to centrally control long-range cyber fires.

Centralized Control

In joint air operations centralized control is giving one commander the responsibility and authority for planning, directing, and coordinating a military operation or group/category of operations. Centralized control facilitates integration of forces to provide guidance, organization, and control to the joint air effort and maintain the ability to focus the impact of joint air forces wherever needed across the operational area. Command relationships are established by the JFC within his command.

—Joint Publication 3-30, *Command and Control of Joint Operations*

As seen in the previous chapter, cyber defense requires C2 to rest in the hands of the commander; however, this is not always the case with cyber attack. The nature of cyberspace includes an environment where commanders must defend against attack on a daily basis and where

²⁴ Editorial, “War in the fifth domain”, *Economist* (1 July 2010), <http://www.economist.com/node/16478792> (accessed 15 May 2012).

small actions beyond the military domain can have grave strategic implications. This nature has identified that “different organizational arrangements may indeed suit different types of war environments and situations,” and “much will depend on the ability of the US military hierarchy to show appropriate judgment and resist the temptation of centralization and micro-management when it is counter-productive.”²⁵ In the case of long-range strategic cyber fires, this management is not counter-productive. Given the strategic nature of offensive action in cyberspace, CYBERCOM, under STRATCOM, should execute cyber attack and exploitation through the SACC and its commander. The SACC will organize, orchestrate, and synchronize long-range strategic cyber attack in support of commanders’ missions. This centralized function is required for two main reasons: the military does not currently hold authorities outside its own networks, and the strategic implications of attacks or errors in cyberspace are significant and still not widely understood. In the following paragraphs, this chapter will analyze two command structures, the JSPOC and the Special Operations Global Mission Support Center, that centrally control forces with strategic implications.

²⁵ Bousquet, *The Scientific Way of Warfare*, 229.

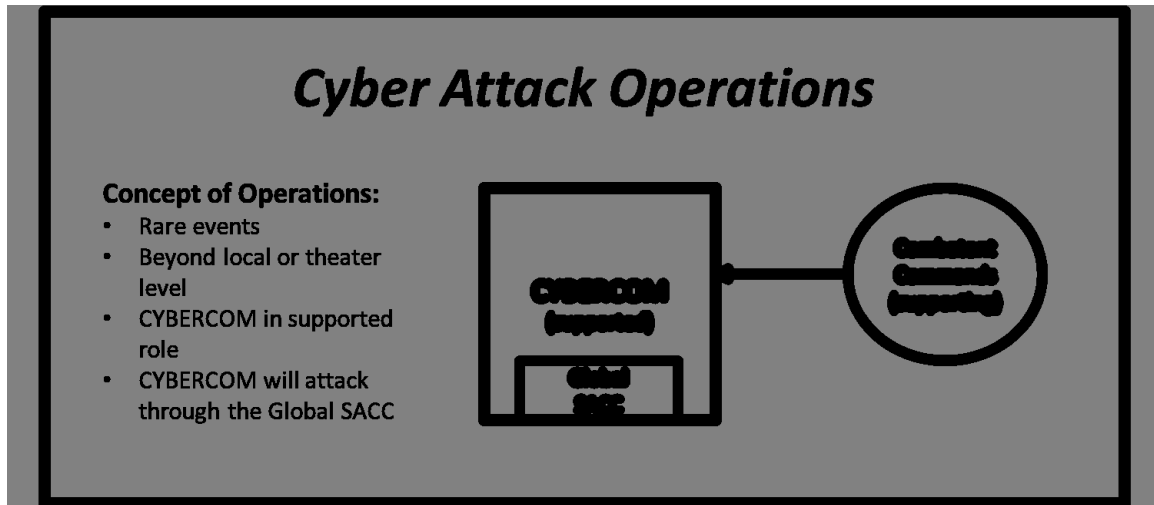


Figure 17: Cyber Attack Operations

Source: Author's Original Work

Special Operations Global Mission Support Center

In a theater of operations military forces “tend to operate as an integrated joint team across the range of military operations using a C2 structure centered on the JFC’s mission and concept of operations, available forces and staff capabilities, location, and facilities.”²⁶ Cyber defense forces, specifically the active defense forces not inherent to a commander’s network are included among these forces. Cyber attack forces, however, are not. This is because cyber attacks are not necessarily specific to the AOR even if the target is. Just as Special Operations Command (SOCOM) has established a Global Mission Support Center as “a single point of entry providing SOF customers a reach-back, push-forward, and think-ahead capability for operational and emerging requirements,” CYBERCOM should establish a single center for strategic cyber attack.²⁷ The JSPOC is one such doctrinal command center that cyber can mirror.

²⁶ JP 3-05, III-2.

²⁷ JP 3-05, III-10.

Joint Space Operation Center

While the JSPOC does not attack in or from space, it does provide strategic effects across the globe, and it does this through a single commander with a single organization at a single location. STRATCOM already holds specific responsibilities for space operations that are applicable, provide a starting point, and can easily be translated into cyberspace operations. A centrally controlled SACC can:

1. Providing warning and assessment of local, theater, or global cyber attack. In the event of a local attack, the Area Cyber Defense Commander (ACDC) can report details up the chain to the SACC, and the SACC can disseminate this information to other AORs.
2. Serving as the single point of contact for military cyber operational matters. The SACC can act as a clearinghouse to disseminate not just attack information, but also a global cyber situational awareness.
3. Providing a military representation to US national agencies, international agencies, and commercial entities for military cyberspace matters as directed and in coordination with the Commander Joint Chiefs of Staff (CJCS) and other Combatant Commanders (CCDRs).
4. Coordinating and conducting cyberspace campaign planning. In the event an ACDC has not yet been established, or an ACDC has identified the need for additional support, the SACC can provide baseline or adjunct planning reinforcements.
5. Setting protection and survivability requirements for cyber capabilities. The SACC will provide the commander of CYBERCOM with the awareness required to set specific global requirement and rules of engagement (ROEs). These may

include passive or active defense measures, or delegated attack measures.²⁸

The CYBERCOM commander, under the STRATCOM commander, will also hold the same cyber responsibilities as the space responsibilities held by the STRATCOM commander in the example of space. These responsibilities include:

1. Plans, integrates, coordinates, and develops desired characteristics and capabilities for global network defense and support for expeditionary network defense.
2. Directs global network operations. These will include sustainment, defensive, and offensive measures.
3. Develops specific cyber courses of action (COA).
4. Provides full support to maintain availability and reliability of Department of Defense (DOD) networks.
5. Plans, directs, coordinates, and controls assigned cyber assets and forces for daily operations and crisis action planning in the event of military action. In addition, provides warning to US national leaders of attacks against cyber assets worldwide, and executes these warning responsibilities through the CDRCYBERCOM and its SACC.²⁹

The mission of the SACC would be to provide the commander of CYBERCOM with the same capabilities that the JSPOC provides the CDR JFCC SPACE: “agile and responsive C2 capabilities to conduct

²⁸ Each of these cyber operations mirror or are directly quoted from the space operations outlined in Section B, “United States Strategic Command and Components,” Joint Publication 3-14, *Space Operations*, (6 January 2009), IV-2.

²⁹ These commander responsibilities mirror or are directly quoted from the CDRSTRATCOM’s responsibilities outlined in Section B, “United States Strategic Command and Components,” and the responsibilities of the Joint Task Force-Global Network Operations. JP 3-14, IV-2, IV-5.

[operations] on a 24/7 basis.”³⁰ Therefore, the SACC will hold the following responsibilities:

1. Provide operational-level cyber C2 support to the CYBERCOM commander.
2. Provide cyber situational awareness and maintain an integrated cyber picture that is shared with commanders and other appropriate cyber users.
3. Plan, direct, control, integrate, and assesses cyberspace operations on behalf of STRATCOM and CYBERCOM.
4. Support inter-theater responsibilities of the ACDC.
5. Develop COAs, plans, and executes cyber operations.
6. Provide day-to-day operations with SACC crews in place to monitor daily events.³¹

Beyond Cyber Attack

Just because offensive cyber attack is separated and centralized at the SACC does not mean that its only focus is offensive operations. The SACC will also provide global defensive situational awareness to combatant commanders through their ACDCs. For example, if one command is being attacked, that information will be shared and specific defense will be identified as the fix that will act as a patch for other vulnerable networks. Attacks and the reactions to an attack will initially be handled by the command being attacked. If their inherent capability does not provide adequate ability to negate the attack, then the ACDC will request additional support from CYBERCOM. Once a fix is identified, the SACC will provide guidance through required defensive measures for the individual commands to implement. In the absence of an ACDC, the SACC can provide guidance and global support at any level

³⁰ JP 3-14, IV-5.

³¹ These roles mirror or are directly quoted from the JSPOC's responsibilities outlined in JP 3-14, IV-2.

of cyber power—sustainment, passive and active defensive measures, and offensive attack. Figure 3 details the measures SACC provides.

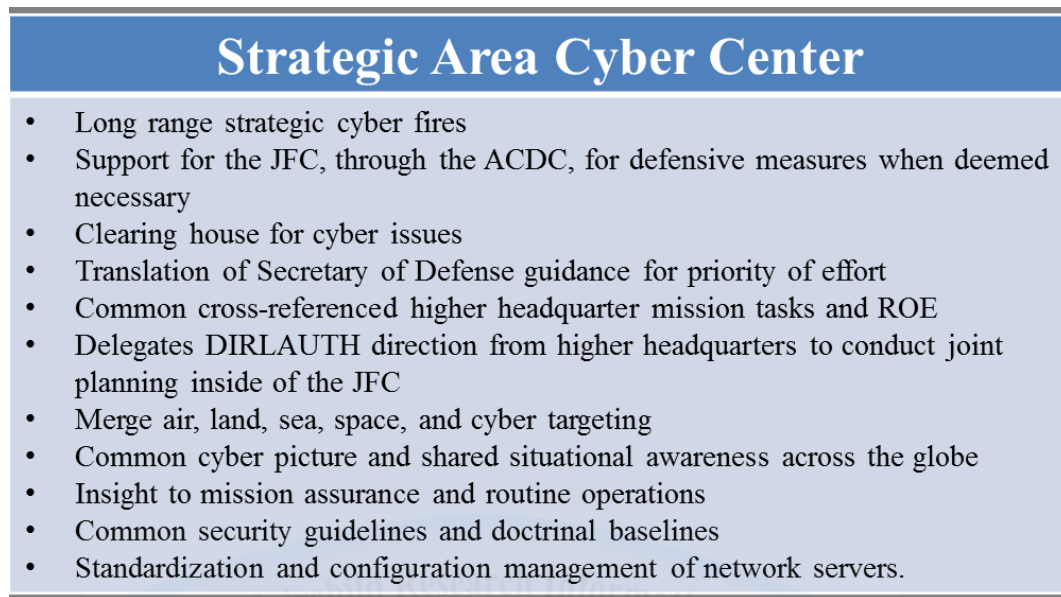


Figure 18: Capabilities Provided by SACC

Source: Author's Original Work

Summary

While cyber defense is necessary to protect the military's networks, cyber offense is necessary for attacking its adversaries. Proper C2 of cyber offense will enable the military to "carry out its proper mission, which is to inflict the maximum amount of death and destruction on the enemy within the shortest possible period of time and at minimum loss to itself."³² Figure 19 shows the level of command and the level of warfare in which cyber attack resides.

³² Martin Van Creveld, *Command in War*, (Cambridge, MA: Harvard University Press, 1985), 6.

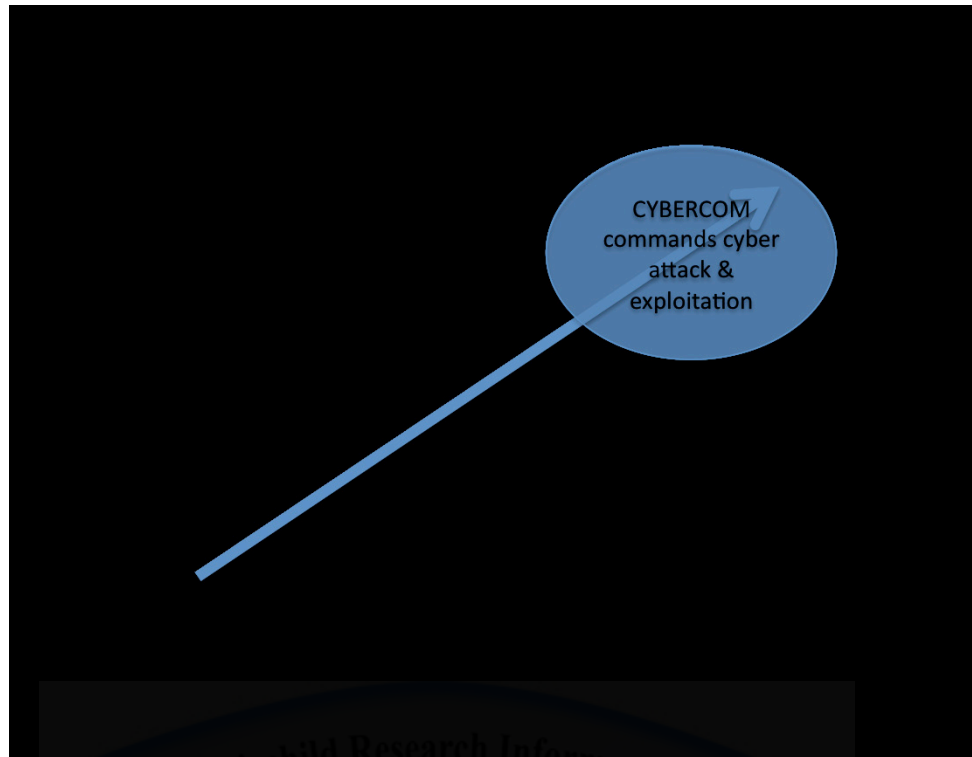


Figure 19: Level of Power—Cyber Attack

Source: Author's Original Work

Operations centers provide commanders with the ability to C2 global operations. The C2 of space and special operations, specifically through the JSPOC and the CDRJSOTF, provide a foundation from which the C2 of cyber can be organized and executed. Because of its strategic implications, the responsibility and authority over cyber attack must sit with CYBERCOM under STRATCOM, and the strategic attack effects must be managed through a single location, the SACC. While the ACDC is responsible for the C2 of cyber forces in theater, and charged with the security of expeditionary networks; the SACC is responsible for the C2 of cyber effects worldwide, and charged with integrating these capabilities for long-range cyber attack.

Conclusion

The first, the supreme, the most far-reaching act of judgment that the statesman and the commander have to make is to establish . . . the kind of war on which they are embarking; neither mistaking it for, nor trying to turn it into, something that is alien to its nature. This is the first of all strategic questions and the most comprehensive.

—Carl von Clausewitz
On War

To use existing technology to the limit and at the same time make its very limitations work for one—surely that is the hallmark of genius.

—Martin van Creveld
Command in War

World War II and the Manhattan Project provided the United States with much more than the technologies that built the hydrogen bomb that ultimately led to the Cold War. The same group of scientists that created the greatest strategic weapon ever known to man also created the computer—a technology whose strategic prowess continues to grow. The innovations and technologies that led to the computer were necessary for the Manhattan Project's research.¹ The computer and cyberspace were both born from military-funded research and innovation.² What followed was a slow explosion of technological advances enabling individuals, businesses, governments, and militaries with information exchange at levels never before thought possible. But it is only now that the military's reliance on cyber has proved necessary to make some significant organizational and command changes in the way it fights war.

¹ This information was taken from an interview of George Dyson, a historian and author of *Turing's Cathedral: The Origins of the Digital Universe*. Kevin Kelly, "The Hacker Historian," (Wired Magazine, March 2012), 94-97.

² Dennis A. Trinkel and Scott A. Merriman, *The American History Highway—A Guide to Internet Resources on US, Canadian, and Latin American History* (Armonk, NY: M.E. Sharpe, Inc., 2007), 3-5.

Cyberspace is a “consensual hallucination.”³ It is an alternate universe created entirely out of the 1s and 0s that make up binary code. The more this technology evolves, the closer human’s physical universe and the 1s and 0s become one. There will not be a digital dictatorship in the future. The digital universe “will always be an undomesticated, unpredictable wilderness.”⁴ Mathematics makes it possible to build code that will do unpredictable things, and the true nature of cyberspace domain will remain—just as the true nature of land, sea, and air domains have remained—a deeply complex and often misunderstood and misapplied environment complete with the same fog and frictions that Clausewitz spoke of some 200 years ago. These complexities combined with actors that intend to steal data or disrupt another’s freedom of action in cyberspace make the cyber environment exceedingly difficult to command and control (C2).

Still, in order to ensure its strategic effectiveness the military must have some sort of control in cyberspace. The Department of Defense (DOD) defines cyberspace as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”⁵ The military must be able to protect its access to this domain, and stop or punish those that would challenge this freedom. The level of control and actual capabilities are what truly matters in military cyberspace action. The military must first secure its own local networks that extend as part of its greater network, the global information grid (GIG). In the case of expeditionary commanders, the responsibility of defense should be inherent in their command forces.

³ William Gibson. *Neuromancer* (New York: The Berkley Publishing Group, 1984), 51

⁴ Kevin Kelly, *The Hacker Historian*, (Wired Magazine, March 2012), 97.

⁵ US Office of the Deputy Secretary of Defense, *The Definition of “Cyberspace,”* Policy Memo, 12 May 2009, in DOD, Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms*, (8 November 2010), 86.

Their network is their fort, and they are in the best position to protect it from would be attackers. Second, the military must retain the capacity to go beyond its castle walls. This will enable exploitation or spying that will gather information, and attacks to thwart an enemy's capabilities. Due to the strategic nature of these offensive actions and the significant implications of "trespassing" in someone's sovereign cyberspace territory, the responsibility must remain centralized at a higher headquarters level.

In *Command in War*, Martin van Creveld explained "the problem of commanding and controlling armed forces . . . is as old as war itself," and this explanation still holds true in cyberspace.⁶ In order to C2 cyber forces properly, one must understand the different levels of cyber power. The figure below separates cyber power between the tactical, operational, and strategic levels of war; and the sustainment, passive defense, active defense, and offensive levels of warfare. As the arrow shows, the more offensive the action in cyberspace, the greater strategic implications it may hold. On the other hand, the more defensive an action, the more decentralized control it may require.

⁶ Martin Van Creveld, *Command in War*, 1.



Figure 20: Levels of Cyber Power

Source: Author's Original Work

Cyber Organization

The history of the American military's cyberspace organization has its origins in information operations (IO) but has only recently settled into the sub-unified Cyber Command (CYBERCOM). This command's mission is to conduct full-spectrum operations in cyberspace, "to defend American military networks and attack other countries' systems."⁷

CYBERCOM lies under the command of Strategic Command (STRATCOM), but the CYBERCOM commander has been deemed important enough to be a four-star general position and is dual-hatted as the director of the National Security Agency (NSA). The incredible amount of cyber attacks against the DOD's networks necessitated a new organization and possibly a new C2 structure. In cyberspace, C2 is can be divided between the offense and the defense. The existing unified

⁷ Editorial, "War in the fifth domain," *Economist*, 3 July 2010, 25.

command plan is the structure in which cyber power is organized. This structure brings all the services into a joint and integrated form, and allows the system to adapt to evolving threats. In the case of cyberspace, the evolving technologies and threats have grown to necessitate a defined C2 structure.

Offense and Defense

Just as Alfred Thayer Mahan explained that the steamship had increased the “scope and the rapidity of naval operation,” cyberspace has accelerated the scope of present military operations, without “necessarily changing the principles” that direct them.⁸ So the nature of cyberspace has not changed the nature of war, but cyberspace does require some specifically structured differences in the C2 of offensive versus defensive measures. In the sporting world it is often said that the offense puts the fans in the seats, but the defense is what really wins the game. This observation has its seed from a centuries old discussion among war strategists: *which is the stronger form of war—the offense or the defense?* The defense establishes one’s foundation, and only through the defense can one begin to think about a prolonged offensive measure. But the defense is not meant to weaken one’s enemy, only protect one’s resources. On the other hand, the offense does attack at the enemy’s resources and is an attempt to put an adversary off balance and tip the balance of power in a conflict. The defense is the stronger form of war, but it is only through the offense that ground can be gained and objectives had beyond what is already established.

The figure below outlines the lines of operation for cyberspace from the defense to the offense. On the left side are those actions to sustain the military’s networks. This includes the establishment and

⁸ Alfred Thayer Mahan, *Mahan On Naval Strategy: Selections from the Writings of Rear Admiral Alfred Thayer Mahan*, ed. John B. Hattendorf (Annapolis, MD: Naval Institute Press, 1991), 8.

maintenance of network infrastructure as well as those passive defense measures required to ensure the network is able to operate as intended. As the lines of operation move from local to theater and global levels, the capabilities gain a more offensive stance. At the theater level, passive and active defense measures are required to sustain one's control in cyberspace. At the global level, which travels beyond one's own network and into an adversary's, cyber exploitation and attack is introduced.



Figure 21: Cyber Lines of Operation
Source: Author's Original Work

Recommendations

Centralized control facilitates integration of forces to provide guidance, organization, and control to the joint air effort and maintain the ability to focus the impact of joint air forces wherever needed across the operational area. Command relationships are established by the JFC within his command. Decentralized execution is the delegation of execution authority to subordinate commanders. This makes it possible to generate the required tempo of operations and to cope with the uncertainty, disorder, and fluidity of combat.

—JP 3-30, *Command and Control of Joint Operations*

Cyberspace does not change the nature of war, but cyber has changed how war should be managed. Cyber power can be divided into two forms of war: the offense and the defense. Offensive cyber, given its strategic nature, must reside at the unified command level. Defensive cyber, on the other hand, given its security nature, must reside at the command level.

The development of cyberspace has not changed the nature of war. What cyberspace has done is change the way offense and defense in war is amplified. The ease of access into this domain has allowed adversaries across the globe to attack America's military networks on a daily basis requiring the command and control of defensive cyber forces to rest in the hands of the individual combatant commander through the area cyber defense commander. The global networked nature of cyberspace has allowed the implications of offensive attack to grow to strategic levels requiring the command and control of offensive cyber forces to rest in the hands of the STRATCOM commander through the CYBERCOM commander. Above all else, the following recommendations will allow JFC's to effectively integrate cyber effects into the land, sea, and air domains.

| Network Maintenance <i>Day-to-Day Sustainment</i> | Network Security <i>Passive & Active Defense</i> | Cyber Attack <i>Long-range Fires</i> |
|---|--|---|
| <ul style="list-style-type: none"> • Inherent communications specialists • Follows Area Cyber Defense Plan (ACDP) established by the ACDC • Implements updates & requirements into existing systems • THREAT: day-to-day cyber threats, viruses, worms, surface hacking | <ul style="list-style-type: none"> • Commanded by the ACDC • Operates out of the theater specific area SACC • Allows a command the ability to fight through cyber attacks • THREAT: onslaught of cyber attacks that cripple cyber support capabilities | <ul style="list-style-type: none"> • CYBERCOM retains authorities for attack or exploitation unless delegated to the ACDC • Operates long range cyber fires from the Global SACC • THREAT: strategic implications & second and third order effects |

Figure 22: Levels of Cyber C2

Source: Author's Original Work

Recommendation 1- Cyber Defense Inherent to the Individual Commander

Military networks are being inundated with cyber attacks, and individual commanders must have inherent capabilities to defend against these barrages. Cyber specialists are required to stop these threats that include viruses, worms, and hacking. These cyber defense specialists will implement updates and requirements into their networks and follow the cyber plan as laid out by the ACDC.

Recommendation 2- Area Cyber Defense Commander

The ACDC will command passive and active defensive measures for the JFC. The implementation of an ACDC will allow for the effective C2 of cyber capabilities under a JFC. This will be accomplished creating different defensive schemes that will ensure the proper planning and execution of passive and active measures. Without defensive measures one's network can be a significant vulnerability highlighting the importance of proper C2 of those actions. Active Defense includes

actions that target and engage a threat, whether inside or outside one's own network. Tactical operations against the enemy will be required in order for commanders to fight through cyber attacks, and these active defensive measures require significant coordination with higher national-level commands.

Recommendation 3- Strategic Area Cyber Center

The strategic implications of military action beyond one's own networks require the highest level of C2. CYBERCOM should retain the authority for long-range cyber fires and network exploitation. In order to effectively C2 these measures CYBERCOM should establish a global command center, or a SACC. From this system, CYBERCOM can receive and disseminate cyber information to and from the COCOMS, and maintain global cyber situational awareness (SA).

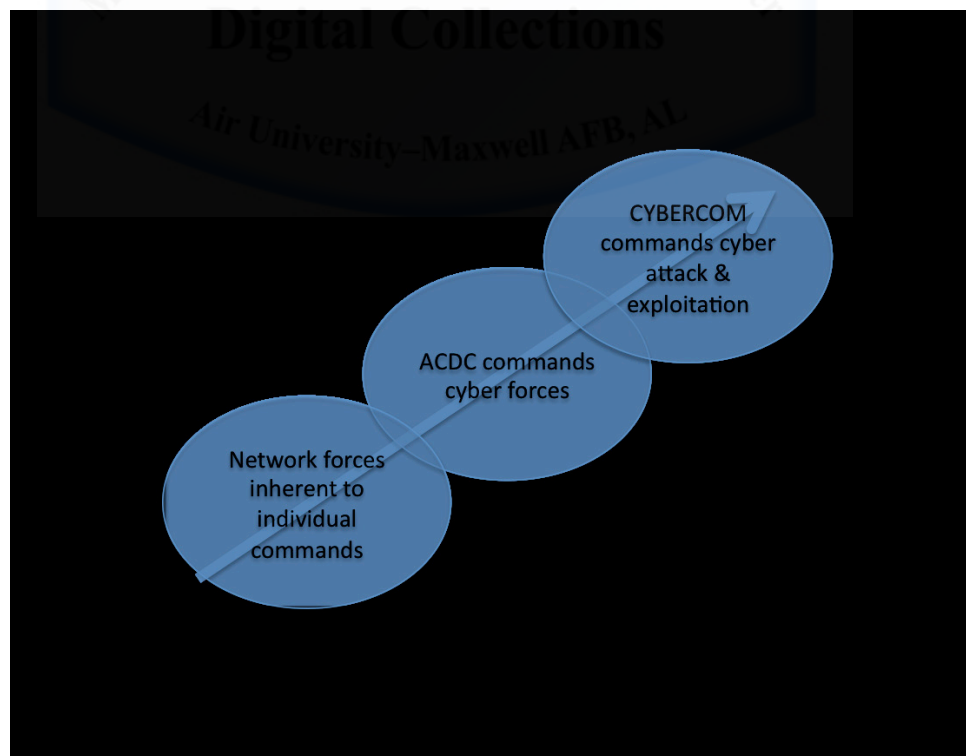


Figure 23: Separate Levels of Cyber Power

Source: Author's Original Work

In conclusion...

C2 of cyber should allow for an effective cyber warfare campaign. Cyber C2 “must identify what cyber resources are available, where they should be allocated, what tasks they should focus on, the risks to friendly cyber resources, the threats from enemy cyber resources, and both tactical and strategical application of friendly cyber resources based on acquired reconnaissance.”⁹ The nature of cyberspace requires a separate command structures for separate cyber missions. The sustainment and defense missions should be localized and theater specific while offensive and strategic missions should remain at the highest levels of command.

Cyberspace demands a new way of war—where commanders anticipate and accept that full spectrum attacks against their networks in an attempt to usurp their cyber and traditional domain capabilities will be commonplace. Commanders should have inherent authorities and capacities to stop these attacks from happening; and they should do this all the while understanding that action beyond their own networks will require strict rules and specific controls often held in a global sense through a single strategic cyber commander.

⁹ Robert F. Erbacher, *Extending Command and Control Infrastructure to Cyber Warfare Assets*, http://www.researchgate.net/publication/4210741_Extending_command_and_control_infrastructures_to_cyber_warfare_assets (accessed 20 January 2012).

BIBLIOGRAPHY

- Air Force Official Website. <http://www.af.mil> (accessed 18 February 2012).
- Air Force Public Website. <http://www.airforce.com> (accessed 19 January 2012).
- Andress, Jason, and Winterfeld, Steve. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Waltham, MA: Syngress, 2011.
- Basla, Michael, Major General, USAF, AFSPACE vice commander. "New Air Force cyberspace badge guidelines release," *Air Force Official Website*, 27 April 2010, <http://www.af.mil/news/story.asp?id=123201885> (accessed 18 January 2012).
- Biddle, Tami Davis. *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas About Strategic Bombing, 1914-1945*, Princeton, NJ: Princeton University Press, 2004.
- Bousquet, Antoine. *The Scientific Way of Warfare—Order and Chaos on the Battlefields of Modernity*. New York: Columbia University Press, 2009.
- Bucci, Steven. "The Confluence of Cyber Crime and Terrorism," for the Heritage Foundation's *Heritage Lectures*, <http://www.insideronline.org/summary.cfm?id=10340> (accessed 20 February 2012).
- Carr, Jeffrey. *Inside Cyber Warfare*, Sebastopol, CA: O'Reilly Books, 2010.
- Carwile, William. "Unified Command and the State-Federal Response to Hurricane Katrina in Mississippi", *Homeland Security Affairs* 1, Article 6 (August 2006), <http://www.hsaj.org/?fullarticle=1.2.6> (accessed 15 February 2012).
- Clarke, Richard A., and Knake, Robert K. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins Publisher, 2010.
- Corbett, Julian S. *Some Principles of Maritime Strategy*. Annapolis, MD: Naval Institute Press, 1988.
- Crucial Point LLC Website. <http://crucialpointllc.com> (accessed 20 February 2012).
- Demchak, Chris C., and Dombrowski, Peter. *Rise of a Cybered Westphalian Age*, *Strategic Studies Quarterly* (Spring 2011).
- Demchak, Chris C. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. Athens, GA: University of Georgia Press, 2011.
- Department of Defense. "2012 Defense Budget Priorities and Choices", Washington D.C., January 2012.
- Department of Defense. "2012 Defense Strategic Guidance—Sustaining U.S. Global Leadership: Priorities for 21st Century Defense," Washington D.C., January 2012.
- Department of Defense. Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms* (8 November 2010).
- Department of Defense. Joint Publication 3-01, *Joint Doctrine for Countering Air and Missile Threats* (19 October 1999).
- Department of Defense, Joint Publication 3-05, *Special Operations* (18 April 2011).
- Department of Defense. Joint Publication 3-13, *Information Operations* (9 October 1998).
- Department of Defense. Joint Publication 3-14, *Space Operations* (6 January 2009).

Department of Defense, Joint Publication 3-30, *Command and Control of Joint Operations* (12 January 2010).

Erbacher, Robert F. *Extending Command and Control Infrastructure to Cyber Warfare Assets*, http://www.researchgate.net/publication/4210741_Extending_command_and_control_infrastructures_to_cyber_warfare_assets, (accessed 20 January 2012).

Fontenot, Jon M., Major, USAF, *A New Era: From SAC to STRATCOM*, (23 May 1995), http://www.fas.org/spp/eprint/fontenot.htm#N_3 (accessed 21 March 2012).

Freedberg, Sydney J. Jr., "Cyber Attacks on Feds Soar 680% in 6 Years: GAO," *America Online Defense* (24 April 2012), <http://defense.aol.com/2012/04/24/cyber-attacks-on-feds-soar-680-in-6-years-gao/> (accessed 24 April 2010).

Gibson, William. *Neuromancer*. New York: The Berkley Publishing Group, 1984.

Global Security Website. <http://www.globalsecurity.org> (accessed 20 February 2012).

Goldwater-Nichols Department of Defense Reorganization Act, Public Law 99-433, 99th Congress, 2nd session. (1 October 1986), 3-4.

Headquarters Air Force, "United States Air Force Posture Statement" (Fiscal Year 2010).

Hughes, Daniel J. (editor). *Moltke—On the Art of War, Selected Writings*, New York: Ballantine Books, 1993.

International Telecommunications Union, "International Communications Technology Facts and Figures". <http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf>, (accessed 20 February 2012).

International Telecommunications Union, "International Communications Technology Statistics". <http://www.itu.int/ITU-D/ict/statistics/> (accessed 20 February 2012).

Internet Movie Database (IMDB), *WarGames*. <http://www.imdb.com/title/tt0086567/>, (accessed 15 January 2012).

Jabbour, Kamal T. Dr., ST. *50 Cyber Questions Every Airman Can Answer*, Air Force Research Laboratory, 7 May 2008.

Johnson, W. Spencer. "New Challenges for the Unified Command Plan," *Joint Forces Quarterly*, (Summer 2002).

Jomini, Antoine-Henri. *The Art of War*, Mineola, N.Y.: Dover Publications, 2007.

Kevin Kelly, Kevin. *The Hacker Historian*, *Wired Magazine* (March 2012).

Kramer, Franklin D., Starr, Stuart H., and Wentz, Larry K. (editors). *Cyberpower and National Security*, Dulles, VA: Potomac Books, Inc.: 2009.

Libicki, Martin C. *Conquest in Cyberspace—National Security and Information Warfare*, New York: Cambridge University Press, 2007.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*, Santa Monica, CA: 2009.

Lonsdale, David J. *The Nature of War in the Information Age*, London: Frank Cass, 2004.

Lord William T., Major General, USAF. "USAF Cyberspace Command: To Fly and Fight in Cyberspace," *Strategic Studies Quarterly* (Fall 2008).

Lynn, William J., III. *Defending a New Domain: The Pentagon's Cyberstrategy*, *Foreign Affairs* (September/October 2010),

- <http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain>, (accessed 15 March 2012).
- Mahan, Alfred Thayer. *Mahan On Naval Strategy: Selections from the Writings of Rear Admiral Alfred Thayer Mahan*, ed. Hattendorf, John B., Annapolis, Md.: Naval Institute Press, 1991.
- McDougall, Walter. *The Heavens and the Earth: A Political History of the Space Age*. Baltimore, MD: The Johns Hopkins University Press.
- Merriman, Scott A., and Trinkel, Dennis A. Trinkel, *The American History Highway—A Guide to Internet Resources on U.S., Canadian, and Latin American History*. Armonk, NY: M.E. Sharpe, Inc., 2007.
- Mitchell, William. *Winged Defense: The Development and Possibilities of Modern Air Power—Economic and Military*. Tuscaloosa, AL: Fire Ant Books, the University of Alabama Press, 2009.
- Morozov, Evgeny. *The Net Delusion—The Dark Side of Internet Freedom*, Philadelphia: PublicAffairs, 2011.
- Murrill, Robert. "The Question of Cyber Terrorism," <http://articles.forensicrofocus.com/2011/07/23/the-question-of-cyber-terrorism/> (accessed 20 February 2010).
- Nakashima, Ellen. "Cyber-intruder Sparks Massive Federal Response—and Debate over Dealing with Threats," *Washington Post*, 8 December 2011, http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html (accessed 14 December 2011).
- Nye, Joseph S. Jr., *The Future of Power*, New York, NY: PublicAffairs, 2011.
- Ratcliff, R.A., *Delusions of Intelligence—Enigma, Ultra, and the End of Secure Ciphers*, New York: Cambridge University Press, 2006.
- Secretary of Defense. "Memorandum from the Secretary of Defense: Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations," *Wall Street Journal*, 23 June 2009, <http://online.wsj.com/public/resources/documents/OSD05914.pdf> (accessed 19 March 2012).
- Sheldon, John B. "Deciphering Cyberpower: Strategic Purpose in Peace and War" in *Strategic Studies Quarterly* (Summer 2011).
- Siegler, M.G. "Eric Schmidt: Every 2 Days We Create As Much Information As We Did Up To 2003," *TechCrunch* (4 August 2010), <http://techcrunch.com/2010/08/04/schmidt-data/> (accessed 15 May 2012).
- Stiennon, Richard. *Surviving Cyber War*, Lanham, MD: Government Institutes, 2010.
- STRATCOM Public Website. <http://www.stratcom.mil> (accessed 22 March 2012).
- Time Magazine Cover Store. <http://www.timecoverstore.com/product/cyber-war-1995-08-21/>, (accessed 15 January 2012).
- U.S. Office of the Deputy Secretary of Defense, *The Definition of "Cyberspace,"* Policy Memo, 12 May 2009
- Van Creveld, Martin. *Command in War*, Cambridge, MA: Harvard University Press, 1985.
- "War in the Fifth Domain", *The Economist* (3 July 2010).
- Wells, H.G. *The War in the Air*. Charleston, SC: BiblioBazaar, 1907.

White House, The. "International Strategy for Cyberspace," May 2011.
White House, The. "The National Strategy to Secure Cyberspace," February 2003.
Wikipedia. <http://en.wikipedia.org> (accessed on multiple dates).

